SuSE Linux

ADMINISTRATIONSHANDBUCH

4. Auflage 2002

Hinweise und Kommentare richten Sie ggf. an documentation@suse.de

Autoren: Frank Bodammer, Stefan Dirsch, Olaf Donjak, Torsten Duwe, Roman Drahtmüller, Thorsten Dubiel, Karl Eichwalder, Thomas Fehr, Stefan Fent, Werner Fink, Carsten Groß, Franz Hassel, Hendrik Vogelsang, Klaus Kämpf, Hubert Mantel, Anas Nashif, Johannes Meixner, Lars Müller, Matthias Nagorni, Peter Pöml, Siegfried Olschner, Marcus Schaefer, Klaus Singvogel, Klaus G. Wagner, Christian Zoz

Redaktion: Antje Faber, Dennis Geider, Roland Haidl, Jana Jaeger, Edith Parzefall, Peter Reinhart, Marc Rührschneck, Thomas Schraitle, Martin Sommer, Rebecca Walter

Layout: Manuela Piotrowski, Thomas Schraitle

Satz: LaTeX

Dieses Buch ist auf 100 % chlorfrei gebleichtem Papier gedruckt.

Inhaltsverzeichnis

Vorwort 1
Neuerungen im Administrationshandbuch 2
Typografische Konventionen 3
Danksagung 4

I Installation **5**

1 Die Installation **7**

Textbasierte Installation mit YaST2 8
Der Startbildschirm 8
Die Grundlage: linuxrc 9
SuSE Linux starten 15
Besondere Installationen 18
Tipps und Tricks 20
Booten von Diskette (SYSLINUX) 20
CD 2 zum Booten verwenden 21
Bootdiskette unter DOS erstellen 21
Bootdiskette unter einem unix-artigen System erstellen 22
Unterstützt Linux mein CD-ROM-Laufwerk? 23
ATAPI-CD-ROM bleibt beim Lesen hängen 24
CD-ROM-Laufwerke am Parallelport 25
loadlin fehlt Speicher, um den Kernel zu laden 26

loadlin funktioniert nicht 26
Partitionieren für Fortgeschrittene 26
Die Größe der Swap-Partition 27
Einsatzgebiet des Rechners 27
Optimierungsmöglichkeiten 29

2 Update des Systems und Paketverwaltung 33
SuSE Linux aktualisieren 34
Vorbereitungen 34
Update mit YaST2 36
Manuell gesteuertes Update 36
Aktualisieren einzelner Pakete 38
Softwareänderungen von Version zu Version 39
Von 6.x auf 7.0 39
Von 7.0 auf 7.1 43
Von 7.1 auf 7.2 44
Von 7.2 auf 7.3 45
Von 7.3 auf 8.0 45
Von 8.0 auf 8.1 47
RPM – Der Paket-Manager der Distribution 48
Prüfen der Authentizität eines Pakets 49
Pakete verwalten: Installieren, Updaten und Deinstallieren 49
Anfragen stellen 51
Quellpakete installieren und kompilieren 54
Tools für RPM-Archive und die RPM-Datenbank 56

II Konfiguration 57

3 YaST2 im Textmodus (ncurses) 59
Erläuterungen zu ncurses 60
Aufruf und Bedienung 60
Bedienung der Module 62
Aufruf der einzelnen Module 63
Das YaST Online Update 63

4 YaST2 im Grafikmodus 65
Der Aufruf von YaST2 66
Software 66
Installationsquelle wechseln 67
YaST Online Update (YOU) 67
Patch-CD-Update 68
Software installieren/löschen 69
Update des Systems 69
Hardware 69
Drucker 69
Anzeige und Eingabegeräte (SaX2) 70
Netzwerk/Basis 70
E-Mail 70
Netzwerk/Erweitert 71
NFS-Server einrichten 72
NIS konfigurieren 72
Hostname und DNS konfigurieren 72
Routing konfigurieren 72
Sicherheit und Benutzer 72
Firewall 73
System 73
LVM 73
Logical Volume Manager (LVM) 74
Soft-RAID 81
Runlevel-Editor 84
Sysconfig-Editor 84
Sonstiges 84

5 Booten und Bootmanager **85**
Der Bootvorgang auf dem PC 86
Bootkonzepte 87
Map Files, LILO und GRUB 88
LILO im Überblick 89
LILO nach Maß 92
Der Aufbau der Datei lilo.conf 93
Weitere optionale Konfigurationsmöglichkeiten 96
Installation und Deinstallation von LILO 100
Beispielkonfigurationen 104
DOS/Windows 95/98 und Linux 104
Windows NT, 2000 oder XP und Linux 105
Probleme mit LILO 107
Booten mit GRUB 107
Das Menü 108
Namen für BIOS-Geräte 109
Installation mit der GRUB-Shell 110
Einrichten des Bootmechanismus mit loadlin 110
Für alle Fälle: Boot-CD erstellen 117
Boot-CD mit ISOLINUX 117

6 Sound mit ALSA **121**
Die grundlegenden PCM-Typen 122
Audiodaten komprimieren 122
Buffering und Latenzen 123
ALSA und Midi 125
MIDI ohne WaveTable-Karte abspielen 131
arecord und aplay 134
Linux für DJs – GDAM und terminatorX 134

7 Hotplug **143**
Realisierung von Hotplug in Linux 144
Hotplug starten und Coldplug 144
USB 145
PCI und PCMCIA 147
Netzwerk 147
Firewire (IEEE1394) 148
Sonstige Geräte und weitere Entwicklung 149

8 Konfiguration und mobiles Arbeiten mit Notebooks **151**
PCMCIA 152
Die Hardware 152
Die Software 152
Die Konfiguration 154
Konfigurationen zum Umschalten – SCPM 156
Wenn's trotzdem nicht geht 157
Installation via PCMCIA 161
Weitere Hilfsprogramme 162
Kernel oder PCMCIA Paket aktualisieren 162
Weiterführende Informationen 163
SCPM – System Configuration Profile Management 164
Grundbegriffe und Grundlagen 164
SCPM YaST2 Modul und weiterführende Dokumentation 165
SCPM einrichten 166
Profile anlegen und verwalten 166
Zwischen Konfigurationsprofilen umschalten 167
Erweiterte Profileinstellungen 168
Profilauswahl beim Booten 170
APM und ACPI – Powermanagement 171
Stromsparfunktionen 172
APM 173
Weitere Befehle 175

ACPI . . . 176
Pause für die Festplatte . . . 177
IrDA – Infrared Data Association . . . 178
Software . . . 179
Konfiguration . . . 179
Verwendung . . . 180
Troubleshooting . . . 180

III System **183**

9 Der Linux Kernel **185**
Kernel-Update . . . 186
Die Kernelquellen . . . 187
Konfiguration des Kernels . . . 187
Kernel-Module . . . 189
Einstellungen bei der Kernelkonfiguration . . . 191
Übersetzen des Kernels . . . 192
Kernel installieren . . . 192
Festplatte nach der Übersetzung aufräumen . . . 194

10 Systemmerkmale **195**
Linux-Standards . . . 196
Filesystem Hierarchy Standard (FHS) . . . 196
Linux Standard Base (LSB) . . . 196
teTeX – TeX unter SuSE Linux . . . 196
Beispiel-Umgebungen für FTP und HTTP . . . 196
Hinweise zu speziellen Softwarepaketen . . . 197
Paket bash und /etc/profile . . . 197
Paket cron . . . 198
Protokoll-Dateien – das Paket logrotate . . . 198
Manual-Pages . . . 200
Der Befehl ulimit . . . 200

Der Befehl free 201
Die /etc/resolv.conf 202
Booten mit der initial ramdisk 202
Konzept der initial ramdisk 203
Ablauf des Bootvorgangs mit initrd 203
Bootloader 204
Anwendung von initrd bei SuSE 205
Mögliche Schwierigkeit – Selbstcompilierte Kernel 206
Ausblick 207
linuxrc 207
Das SuSE Rettungssystem 212
Vorbereitung 214
Das Rettungssystem starten 215
Das Rettungssystem benutzen 216
Virtuelle Konsolen 219
Tastaturbelegung 219
Lokale Anpassungen – I18N/L10N 220

11 Das Bootkonzept **225**
Das init-Programm 226
Die Runlevels 226
Wechsel des Runlevels 228
Die Init-Skripten 229
Der YaST2 Runlevel-Editor 232
SuSEconfig, /etc/sysconfig und /etc/rc.config 233
Systemkonfiguration mit dem YaST2 Sysconfig-Editor 235
Skripte und Variablen – Konfiguration des Systems 235

IV Netzwerk 267

12 Grundlagen der Vernetzung 269

TCP/IP - Das von Linux verwendete Protokoll 270

Schichtenmodell 271

IP-Adressen und Routing 274

Domain Name System 277

IPv6 – Internet der nächsten Generation 278

Warum ein neues Internet-Protokoll? 278

Aufbau einer IPv6-Adresse 280

IPv6-Netzmasken 282

Weiterführende Literatur und Links zu IPv6 283

Die Einbindung ins Netzwerk 284

Vorbereitungen 284

Konfiguration mit YaST2 284

Hotplug/PCMCIA 286

Konfiguration von IPv6 287

Manuelle Netzwerkkonfiguration 287

Konfigurationsdateien 289

Startup-Skripten 295

Routing unter SuSE Linux 296

DNS – Domain Name Service 297

Nameserver BIND starten 297

Die Konfigurationsdatei /etc/named.conf 299

Weitere Informationen 306

NIS – Network Information Service 307

NIS-Master- und -Slave-Server 307

Das NIS-Client-Modul im YaST2 309

Manuelles Einrichten eines NIS-Clients 310

NFS – verteilte Dateisysteme 312

Importieren von Dateisystemen mit YaST2 312

Manuelles Importieren von Dateisystemen 313

Exportieren von Dateisystemen mit YaST2 313
Manuelles Exportieren von Dateisystemen 313
DHCP 317
Das DHCP-Protokoll 317
DHCP-Softwarepakete 317
Der DHCP-Server dhcpd 318
Rechner mit fester IP-Adresse 320
Weitere Informationen 321

13 Heterogene Netzwerke **323**
Samba 324
Installation und Konfiguration des Servers 325
Samba als Anmelde-Server 329
Installation der Clients 330
Optimierung 331
Netatalk 332
Konfiguration des Fileservers 333
Konfiguration des Druckservers 337
Starten des Servers 337
Netware-Emulation mit MARSNWE 339
Netware Emulator MARSNWE starten 339
Die Konfigurationsdatei /etc/nwserv.conf 339
Zugriff auf Netware-Server und deren Administration 342
IPX-Router mit ipxrip 343

14 Internet **345**
Konfiguration eines ADSL / T-DSL Anschlusses 346
Standardkonfiguration 346
DSL Verbindung per Dial-on-Demand 346
Proxy-Server: Squid 347
Was ist ein Proxy-Cache? 348
Informationen zu Proxy-Cache 348
Systemanforderungen 350

Squid starten . . . 352
Die Konfigurationsdatei /etc/squid.conf . . . 354
Transparente Proxy-Konfiguration . . . 359
Squid und andere Programme . . . 362
Weitere Informationen zu Squid . . . 367

V Anhänge **369**

A Dateisysteme unter Linux **371**
Glossar . . . 371
Die wichtigsten Dateisysteme unter Linux . . . 372
Ext2 . . . 372
Ext3 . . . 373
ReiserFS . . . 374
JFS . . . 375
XFS . . . 376
Weitere unterstützte Dateisysteme . . . 377
Large File Support unter Linux . . . 378
Weitere Informationen . . . 379

B Manual-Page von e2fsck **381**

C Deutsche Übersetzung der GNU General Public License **387**

Literaturverzeichnis **399**

Vorwort

In [SuS02b] haben Sie erfahren, wie einfach es ist, Ihr neues SuSE Linux zu installieren und zu bedienen, wie Sie Ihre Hardware einrichten und Software installieren, wie verschiedene Programme bedient werden und wo Sie schnelle Hilfe erhalten. Hier halten Sie nun das neue *Administrationshandbuch* in den Händen. Erfahrene SuSE Linux-Benutzer kennen den Vorgänger dieses Buches wahrscheinlich unter dem Titel *Die Referenz*.

Mit diesem Buch steigen Sie in die Technik von SuSE Linux ein und erfahren Details zur Systemadministration und zur Konfiguration spezieller Systemteile. Außerdem lernen Sie einiges zu den theoretischen Grundlagen bestimmter Eigenheiten von Linux und speziell von SuSE Linux. So erhalten Sie z. B. Hintergrundinformationen zum X-Window-System, zum Bootkonzept, zum Drucken unter Linux oder zum Kernel.

Die Arbeit mit und in Netzwerken ist schon immer eine der großen Stärken von Linux. Daher haben wir der Theorie, Einrichtung und Administration von Netzwerken mit ihren unterschiedlichen Protokollen und Diensten einen Großteil des Buches gewidmet. So erfahren Sie eine Menge über verschiedene Protokolle, über Rounting, NFS und NIS, über heterogene Netze mit Samba und Netatalk sowie über Proxies und den Webserver Apache. Den Abschluss bildet schließlich ein ausführliches Kapitel über das heikle Thema Sicherheit und deren Gewährleistung in Netzwerken.

Neulinge mögen bisweilen etwas vor dem Inhalt des Buches zurückschrecken, aber auch interessierte Einsteiger werden beim Schmökern in diesem Buch vieles entdecken, was gar nicht so schwer verständlich ist und den technischen Horizont bedeutend erweitern wird. Sie werden womöglich entdecken, dass Ihr SuSE Linux, beginnend bei der Idee des Open Source-Gedankens über das Bootkonzept und die einfache Installation bis hin zum stabilen und sicheren Netzwerkbetrieb und der extrem flexiblen X11-Umgebung, einfach das bessere Betriebssystem ist!

Neuerungen im Administrationshandbuch

In diesem Abschnitt finden Sie eine Auflistung der Änderung an der Dokumentation von der letzten zur aktuellen Version:

- Aufgrund vieler Neuerungen wurden folgende Kapitel stark überarbeitet:
  - Anpassung des Kapitel *Das Bootkonzept* auf Seite 225 an die aktuelle Version (Variablen, `/etc/sysconfig` usw.)
  - YaST2: Komplexe Teile wurden vom Benutzerhandbuch in das Administrationshandbuch verschoben.
  - Drucken über CUPS und im TCP/IP-Netzwerk (siehe Seite **??**)
- Neu hinzu kamen folgende Kapitel:
  - GRUB, ein alternativer Bootmanager (siehe Seite 107).
  - Ein Kapitel über die Besonderheiten von Laptops wurde aufgenommen (siehe Seite 151).
  - Hotplug, wie Sie Computer-Hardware zur Laufzeit des System an- oder aushängen (siehe Seite 143).
  - Kerberos, ein Authentifizierungsmechanismus (siehe Seite **??**).
  - Vergleich von Dateisystemen unter Linux (siehe Seite 371).

Typografische Konventionen

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

Auszeichnung	Bedeutung
YaST	die Angabe eines Programmnamens
`/etc/passwd`	die Angabe einer Datei oder eines Verzeichnisses
⟨*platzhalter*⟩	die Zeichenfolge `platzhalter` (inkl. Winkelklammern) ist durch den tatsächlichen Wert zu ersetzen
`PATH`	eine Umgebungsvariable mit dem Namen `PATH`
`192.168.1.2`	der Wert einer Variablen
`ls`	die Angabe eines einzugebenden Befehls
`user`	die Angabe eines Benutzers
`erde:~ #` **`ls`**	Eingabe von `ls` auf der Shell des Benutzers `root` im Homeverzeichnis auf dem Rechner „Erde“
`tux@erde:~ >` **`ls`**	Eingabe von `ls` auf der Shell des Benutzers `tux` (offizieller Name des Linux-Pinguins) im Homeverzeichnis auf dem Rechner „Erde“
`C:\>` **`fdisk`**	DOS-Prompt mit der Befehlseingabe `fdisk`
(Alt)	eine zu drückende Taste; nacheinander zu drückende Tasten werden durch Leerzeichen getrennt
(Ctrl) + (Alt) + (Entf)	gleichzeitig zu drückende Tasten werden durch `'+'` miteinander verbunden
"Permission denied"	Meldungen des Systems
‘System updaten’	Menü-Punkte, Buttons
Booten	Verweist auf einen Eintrag im Glossar im Anhang
„DMA-Modus“	Namenskonventionen, -definitionen, Sogenanntes…

Danksagung

Die Liste mit allen, die zum Gelingen dieser Distribution beigetragen haben, hier aufzuführen, würde alleine ein Buch füllen. Daher danken wir hier pauschal allen, die mit unermüdlichem Einsatz dafür gesorgt haben, dass Sie auch diesmal wieder ein ausgezeichnetes SuSE Linux vor sich haben, das alle bisherigen übertrifft.

Die Entwickler von Linux treiben in weltweiter Zusammenarbeit mit hohem freiwilligen Einsatz das Werden von Linux voran. Wir danken ihnen für ihr Engagement – ohne sie gäbe es diese Distribution nicht.

Nicht zuletzt geht unser besonderer Dank selbstverständlich an Linus Torvalds!

Have a lot of fun!

Ihr SuSE Team

Teil I

Installation

Die Installation

SuSE Linux lässt sich je nach lokalen Erfordernissen flexibel installieren; die Varianten reichen von einer manuell gesteuerten bis zu einer voll automatisierten Installation.

Im Folgenden finden Sie verschiedene Installationsvarianten wie z. B. die textbasierte Installation mit YaST2, Hinweise zur Verwendung unterschiedlicher Installationquellen (CD-ROM, FTP, NFS) und zur automatisierten Installation. Die ausführliche Beschreibung der grafischen Standardinstallation finden Sie am Anfang des Benutzerhandbuchs.

Den Abschluss dieses Kapitels bilden Tipps zu Problemen bei der Installation sowie Anleitungen zu deren Behebung.

Textbasierte Installation mit YaST2 8
SuSE Linux starten 15
Besondere Installationen 18
Tipps und Tricks 20
Partitionieren für Fortgeschrittene 26

Hinweis

Hier im Administrationshandbuch finden Sie nur besondere Installationsvarianten. Die ausführliche Beschreibung der grafischen Standardinstallation finden Sie zu Beginn des Benutzerhandbuchs.

Hinweis

Textbasierte Installation mit YaST2

Hintergrundinfo

Zusätzlich zur Installation mit grafischer Benutzerführung kann SuSE Linux auch mithilfe der Textmenüs von YaST2 installiert werden (Konsolenmodus). Alle YaST2-Module stehen auch in diesem Textmodus zur Verfügung. Der Textmodus kann insbesondere dann eingesetzt werden, wenn man keine grafische Oberfläche benötigt (Serversysteme) oder wenn die Grafikkarte von dem X Window System nicht unterstützt wird. Selbstverständlich werden Blinde, die auf ein textuelle Schnittstelle angewiesen sind, auch diesen Textmodus verwenden.

Der Startbildschirm

Legen Sie die CD 1 in das Laufwerk und starten Sie den Rechner neu. Falls der Rechner nicht booten will, müssen Sie zuvor möglicherweise die Bootreihenfolge im BIOS des Rechners auf `CDROM,C,A` umstellen.

Nach wenigen Augenblicken wird der Startbildschirm angezeigt. Wählen Sie innerhalb von 10 Sekunden 'Manual Installation', damit *nicht* automatisch YaST2 gestartet wird. Geben in der Zeile `boot options` Bootparameter ein, falls Ihre Hardware derartige Parameter verlangt – in der Regel sind derartige Parameter nicht erforderlich. Mit dem Parameter `textmode=1` können Sie erzwingen, dass der gesamte Bildschirm im Textmodus von YaST2 ausgenutzt wird. Wählen Sie [F2=Text] um in den Textmodus zu gelangen – falls gewünscht – und drücken Sie [↵].

Nun erscheint eine Box mit der Fortschrittsanzeige "Loading Linux kernel"; dann bootet der Kernel und linuxrc wird gestartet.

Das Programm linuxrc ist menügeführt und wartet auf Eingaben des Benutzers.

Mögliche Probleme

- Sollte Ihr CD-ROM-Laufwerk (ATAPI) beim Booten des Systems hängenbleiben, vergleichen Sie bitte den Abschnitt *ATAPI-CD-ROM bleibt beim Lesen hängen* auf Seite 24.
- Die CD 1, die einen optimierten Kernel für Pentium-Prozessoren aufweist, wird nicht als Bootmedium erkannt. Versuchen Sie, auf die „Bootdisk" oder auf CD 2 auszuweichen; vgl. die Abschnitte *Booten von Diskette (SYSLINUX)* auf Seite 20 bzw. *CD 2 zum Booten verwenden* auf Seite 21.
- Bei Grafikkarten wie FireGL 1, 2 oder 3 wird nicht im grafischen Modus (Framebuffer) gestartet. Die Installation muss in diesem Fall im Textmodus durchgeführt werden.
- Andere Boot-Schwierigkeiten können in der Regel mit Kernel-Parametern umgangen werden. Für die Fälle, bei denen DMA Schwierigkeiten bereitet, wird die Startoption 'Installation - Safe Settings' angeboten.
- Wählen Sie 'Memory Test', um den Speicher zu überprüfen, wenn es beim Laden des Kernels oder im Verlauf der Installation zu „unerklärlichen" Schwierigkeiten kommt. Linux stellt hohe Anforderungen an die Hardware und der Speicher und dessen Timing muss einwandfrei eingestellt sein! Mehr Info unter:

  `http://sdb.suse.de/de/sdb/html/thallma_memtest86.html`

  Lassen Sie den Speichertest am besten über Nacht laufen.

Die Grundlage: linuxrc

Mit dem Programm linuxrc können Sie Einstellungen zur Installation vornehmen. Falls notwendig können Sie Treiber als Kernelmodule laden. Am Ende wird linuxrc das Installationsprogramm YaST starten, und die eigentliche Installation der Systemsoftware und der Programme kann beginnen.

Hinweise zur Bedienung von linuxrc: Mit ↑ und ↓ wählen Sie einen Menüpunkt, und mit ← und → wählen Sie ein Kommando aus, etwa 'Ok' oder 'Abbruch'. Mit ↵ wird das Kommando ausgeführt.

Eine genaue Beschreibung von linuxrc finden Sie in Abschnitt *linuxrc* auf Seite 207 ff.

Einstellungen

Das Programm linuxrc beginnt mit der Sprach- und Tastaturauswahl.

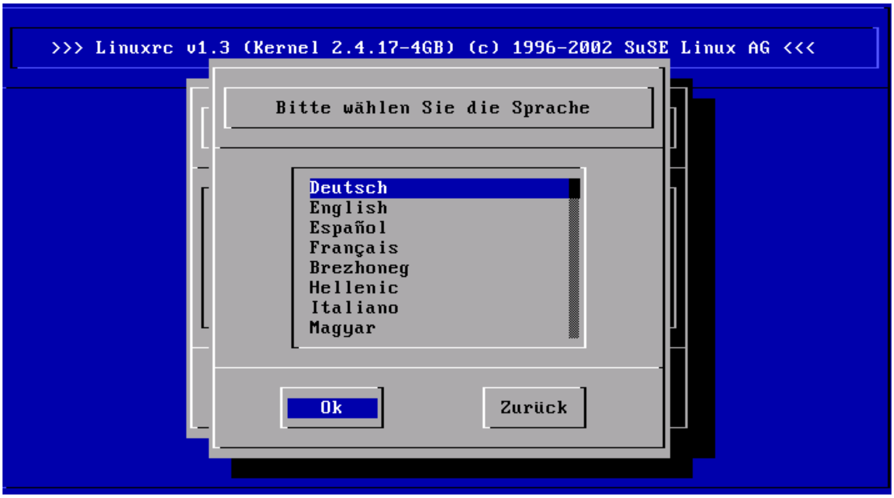


Abbildung 1.1: Auswahl der Sprache

- Wählen Sie die Sprache für die Installation aus (z. B. 'Deutsch') und bestätigen Sie mit ⏎ .
- Wählen Sie dann die Tastaturbelegung (z. B. 'Deutsch').

Mögliche Probleme

- linuxrc bietet die gewünschte Tastaturbelegung nicht an. In einem solchen Fall wählen Sie zunächst eine alternative Belegung (Notnagel: 'English (US)'); nach der Installation kann später auf die genaue Belegung mit YaST umgeschaltet werden.

Hauptmenü von linuxrc

Jetzt sind wir im Hauptmenü von linuxrc (Abbildung 1.2 auf der nächsten Seite).

Hier gibt es folgende Optionen:

'Einstellungen' Hier können Sie Sprache, Bildschirm oder Tastatur anpassen. Das hatten wir bereits.

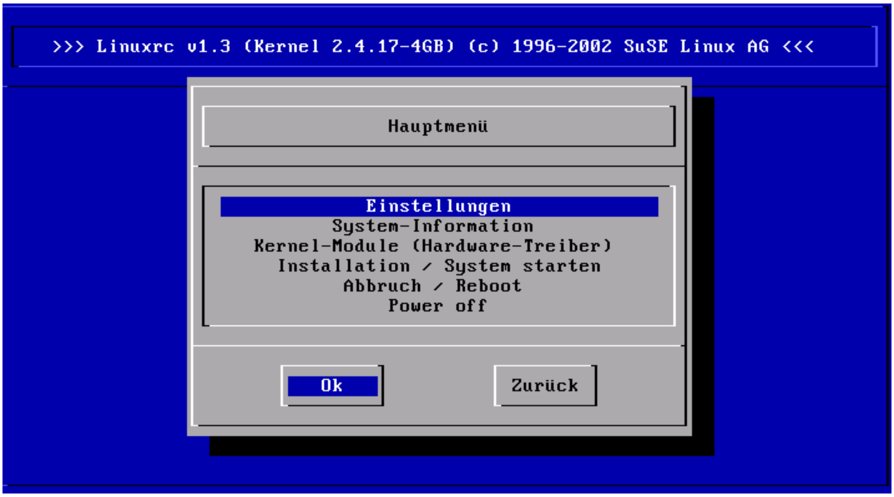


Abbildung 1.2: *Hauptmenü von linuxrc*

'System-Information' Hier gibt es eine Menge Informationen über die Hardware, soweit diese vom Kernel erkannt wurde oder von bereits geladenen Modulen angesprochen wird.

'Kernel-Module (Hardware-Treiber)' Hier müssen Sie eventuell die zur Hardware passenden Module laden. Zudem verstecken sich hier zusätzlich zu ladende Dateisysteme (ReiserFS!).

Regelfall: Sie müssen diesen Menüpunkt *nicht* aufrufen, wenn Sie sowohl Festplatte(n) als auch das CD-ROM-Laufwerk (ATAPI) an einem (E)IDE-Controller angeschlossen haben; denn die (E)IDE-Unterstützung ist nämlich fest in den Kernel eingebaut.

'Installation/System starten' Hier wird die Installation fortgesetzt.

'Abbruch/Reboot' Falls Sie sich nochmal alles anders überlegen...

'Power off' Um das System anzuhalten und vom Strom zu nehmen.

Einbindung der Hardware über Module

Wählen Sie das Laden der Kernelmodule über den Menüpunkt 'Kernel-Module' dann, wenn Sie Unterstützung für spezielle Systemmerkmale benötigen. Traditionell ist dies für SCSI, Netzwerkkarten oder PCMCIA der

Fall oder wenn das CD-ROM-Laufwerk, von dem installiert werden soll, *kein* ATAPI-Laufwerk ist; mittlerweile sind aber auch andere Komponenten als Modul ausgelagert (z. B. IDE) bzw. neu hinzugekommen (z. B. USB, FireWire oder Dateisysteme).

Wie Sie Module laden, können Sie in Abschnitt *linuxrc* auf Seite 207 nachlesen. Im folgenden Untermenü wählen Sie aus, wofür Sie Module laden wollen (oder besser gesagt: laden müssen). Es kommen in Frage:

Ein SCSI-Modul wenn Sie eine SCSI-Festplatte oder SCSI-CD-ROM-Laufwerk haben.

Ein CD-ROM-Modul falls Ihr CD-ROM-Laufwerk *nicht* am (E)IDE-Controller oder *nicht* am SCSI-Controller hängt.

Ein Netzwerk-Modul falls Sie über NFS oder FTP installieren wollen – das ist hier aber nicht das Thema; vgl. Abschnitt 1 auf Seite 18.

Ein oder mehrere Dateisysteme z. B. ReiserFS oder ext3.

Tipp

Wenn Sie Support für Ihr Installationsmedium (proprietäres CD-ROM-Laufwerk, Parallelport-CD-ROM-Laufwerk, Netzwerkkarte, PCMCIA) unter den Standard-Modulen vermissen, können Sie eventuell auf die zusätzlichen Treiber einer Modules-Diskette zurückgreifen; zum Erstellen einer solchen Diskette vgl. *Bootdiskette unter DOS erstellen* auf Seite 21. Gehen Sie bis ans Ende der Liste und wählen Sie dort den Punkt '-- Weitere Module --'; die Modules-Diskette wird von linuxrc in diesem Fall angefordert.

Tipp

Installation starten

Da 'Installation/System starten' bereits ausgewählt ist, brauchen Sie nur noch ↵ zu drücken, um zur eigentlichen Installation zu gelangen.

Hier stehen folgende Punkte zur Auswahl:

'Installation/Update starten' Das, was Sie vermutlich gleich machen werden.

'Installiertes System booten' Dieser Punkt wird eventuell später einmal benötigt, falls es zu Problemen beim regulären Booten kommen sollte.

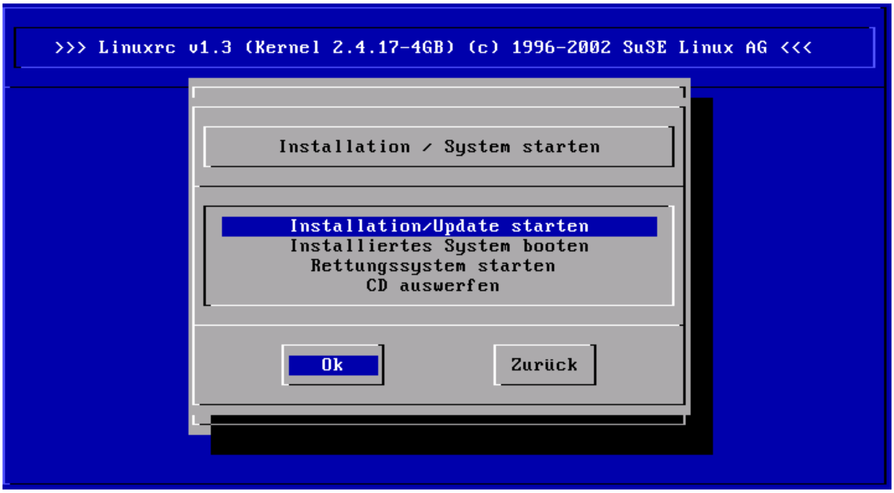


Abbildung 1.3: *Installationsmenü von* linuxrc

'Rettungssystem starten' Dieser Punkt steht bislang nur auf X86-kompatiblen Systemen zur Verfügung.

'CD auswerfen' CD auf elektronischem Wege herauswerfen.

Um zur Installation zu gelangen, drücken Sie nun ↵ für den Menüpunkt 'Installation/Update starten'. Dann muss das Quellmedium ausgewählt werden; in der Regel reicht es aus, den Cursor an der Vorauswahl stehen zu lassen: 'CD-ROM'.

Drücken Sie nun ↵. Es wird die Installationsumgebung direkt von der CD 1 gestartet.

Sobald dieser Vorgang abgeschlossen ist, startet YaST2 in der Version mit der Textoberfläche (ncurses). Die Installation geht dann inhaltlich weiter, wie in [SuS02a], Kapitel *Installation*.

Mögliche Probleme

- Der verwendete SCSI-Adapter wird nicht erkannt:
  - Versuchen Sie, das Module eines kompatiblen Treibers zu laden.
  - Verwenden Sie einen Kernel, der den entsprechenden SCSI-Treiber fest hinzugebunden hat; erstellen Sie eine derartige Boot-Diskette,

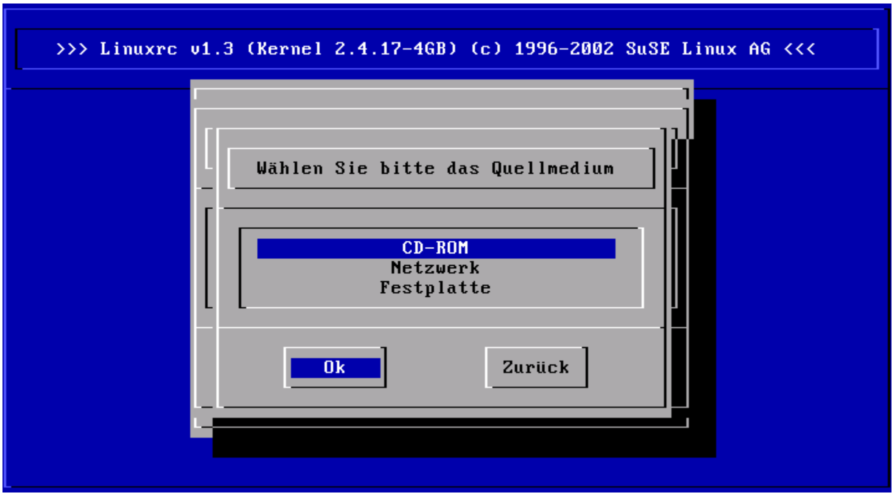


Abbildung 1.4: *Quellmedium in* linuxrc *auswählen*

wie in Abschnitt *Bootdiskette unter DOS erstellen* auf Seite 21 beschrieben.

- Das verwendete ATAPI-CD-ROM-Laufwerk bleibt beim Lesen hängen: siehe Abschnitt *ATAPI-CD-ROM bleibt beim Lesen hängen* auf Seite 24.

- Unter bislang ungeklärten Umständen kann es zu Problemen beim Laden der Daten in die RAM-Disk kommen, sodass YaST nicht geladen werden kann. Meistens führt in diesen Fällen der folgende Weg zu einem brauchbaren Ergebnis:

  Wählen Sie im linuxrc-Hauptmenü 'Einstellungen' → 'Debug (Experte)'; dort stellen Sie 'Erzwinge Rootimage' (engl. *Force root image*) auf `nein` (engl. *no*). Gehen Sie zurück ins Hauptmenü und beginnen Sie die Installation erneut.

SuSE Linux starten

Nach der Installation bleibt die Frage zu klären, wie Sie Linux im täglichen Betrieb starten wollen (Booten).

In der folgenden Übersicht werden die verschiedenen Alternativen für einen Linux-Start vorgestellt; welche dieser Startmethoden für Sie die beste ist, hängt vornehmlich von dem vorgesehenen Verwendungszweck ab.

Bootdiskette Sie starten Linux über die *Bootdiskette* („Startdiskette"). Diese Möglichkeit funktioniert immer und macht keine Arbeit – die Bootdiskette wurde möglicherweise während der Installation mit YaST2 nebenbei erzeugt.

Die Bootdiskette ist eine gute Zwischenlösung, falls Sie beim Einrichten der anderen Möglichkeiten nicht sofort zurechtkommen oder falls Sie die Entscheidung über den endgültigen Bootmechanismus verschieben wollen. Auch im Zusammenhang mit OS/2 oder Windows NT mag die Bootdiskette eine Lösung darstellen.

loadlin Die loadlin-Variante setzt voraus:

- Der Rechner muss unter DOS entweder im Realmodus laufen oder im Virtuellen 8086-Modus einen VCPI-Server verfügbar haben; ein VCPI-Server wird z. B. von emm386.exe zur Verfügung gestellt. Anders gesagt: dieser Weg funktioniert *nicht* unter Unix, OS/2, Windows NT oder im DOS-Fenster von Windows 95/98 – er funktioniert aber gut vom DOS-Prompt oder vom DOS-Modus in MS Windows 95/98 aus.
- Ihr Rechner muss ausreichend freien Speicher haben, der unter DOS verfügbar ist: unterhalb 640 KB mindestens 128 KB, der Rest darf extended/EMS/XMS Speicher sein.

Zwar ist loadlin vergleichsweise aufwendig in der Installation, aber dann lässt es sich ausgezeichnet in die Bootmenüs von Windows 95/98 integrieren. Dies erfordert ein manuelles Editieren von Konfigurationsdateien. Ein großer Vorteil ist, dass keinerlei Einträge in den MBR (engl. *Master Boot Record*) der Festplatte erfolgen; so sehen andere Betriebssysteme von Linux nur Partitionen mit für sie unbekannten Kennungen (engl. *IDs*).

Um loadlin zu installieren, benötigen Sie gewisse Kenntnisse von DOS und Linux. Sie sollten in der Lage sein, mit einem Editor die notwendigen Konfigurationsdateien zu erstellen. Details zum Vorgehen finden Sie in Abschnitt *Einrichten des Bootmechanismus mit loadlin*

auf Seite 110. Schwierigkeiten können sich ergeben, wenn Sie bei der Konfiguration der Windows 95/98-Bootmenüs einen Fehler machen. Im Extremfall kann dies dazu führen, dass Sie nicht mehr an Ihre Windows-Installation herankommen. *Vor* der Konfiguration dieser Bootmenüs sollten Sie sicherstellen, dass Sie Ihr System über eine Windows-Bootdiskette starten können.

Linux Bootloader Die technisch sauberste und universellste Lösung ist die Verwendung eines Linux Bootmanagers, wie LILO (LInux LOader) oder GRUB, die vor dem Booten die Auswahl zwischen verschiedenen Betriebssystemen zulassen. Der Bootloader kann entweder bereits während der Installation eingerichtet oder später z. B. über YaST konfiguriert werden.

Achtung

Es gibt BIOS-Varianten, die die Struktur des Bootsektors (MBR) überprüfen, und nach einer LILO-Installation fälschlich eine Virus-Warnung mitteilen. Diese Schwierigkeit lässt sich leicht beheben, indem Sie in das BIOS gehen und nach derartigen Einstellungsmöglichkeiten dort suchen; z. B. sollten Sie 'Virus Protection' ausschalten. – Später können Sie diese Option wieder einschalten; dieses Feature ist allerdings überflüssig, falls Sie ausschließlich Linux als Ihr Betriebssystem verwenden.

Achtung

Eine eingehende Diskussion verschiedener Bootmethoden, insbesondere aber von LILO, GRUB und loadlin finden Sie in Kapitel 5 auf Seite 85 ff.

Der grafische SuSE-Bildschirm

Seit SuSE Linux 7.2 wird auf Konsole 1 der grafische SuSE-Bildschirm dargestellt, wenn als Kernel-Parameter die Option "vga=771" aktiv ist; bei der Installation mit YaST2 wird diese Option automatisch eingetragen.

SuSE-Bildschirm deaktivieren

Prinzipiell haben Sie drei Möglichkeiten:

- Den SuSE-Bildschirm bei Bedarf deaktivieren.

  Tippen Sie

  ```
  erde:~ #  echo 0 >/proc/splash
  ```

auf der Kommandozeile ein, um den grafischen Bildschirm auszuschalten. Durch folgenden Befehl lässt er sich wieder einschalten:

```
erde:~ #  echo 0x0f01 >/proc/splash
```

- Den SuSE-Bildschirm standardmäßig deaktivieren:

  Fügen Sie der Bootloader-Konfiguration einen Kernelparameter `splash=0` hinzu. Im Kapitel *Booten und Bootmanager* auf Seite 85 finden Sie nähere Informationen dazu. Falls Sie ohnehin lieber den Textmodus wünschen, der bei früheren Versionen Standard war, setzen Sie alternativ `"vga=normal"` .

- Den SuSE-Bildschirm für immer deaktivieren:

  Kompilieren Sie einen neuen Kernel und deaktivieren Sie die Option `Use splash screen instead of boot logo` im Menu 'framebuffer support'.

Tipp

Wenn Sie im Kernel den Framebuffer-Support deaktiviert haben, ist der „Splash-Screen“ automatisch auch deaktiviert. Wenn Sie einen eigenen Kernel kompilieren, kann SuSE dafür keinen Support garantieren!

Tipp

Besondere Installationen

Installation ohne CD-ROM-Unterstützung

Was tun, wenn eine Standard-Installation via CD-ROM-Laufwerk nicht möglich ist? Ihr CD-ROM-Laufwerk könnte z. B. nicht unterstützt werden, weil es sich um ein älteres „proprietäres“ Laufwerk handelt. Oder Sie haben bei Ihrem Zweitrechner (z. B. ein Notebook) eventuell gar kein CD-ROM-Laufwerk, aber dafür einen Ethernet-Adapter oder ein PLIP-Kabel. . .

SuSE Linux bietet die Möglichkeit, auf einem solchen Rechner ohne CD-ROM-Unterstützung über eine Netz-Verbindung zu installieren: NFS oder FTP via Ethernet oder via PLIP (Abschnitt *Installation von einer Quelle im „Netz“* auf dieser Seite) stehen zur Verfügung.

Installation von einer Quelle im „Netz“

Für diesen Weg kann kein Installationssupport in Anspruch genommen werden. Nur erfahrene Computer-Benutzer sollten ihn beschreiten.

Worum geht es?

Der Rechner, auf dem SuSE Linux installiert werden soll, verfügt über *kein* CD-ROM-Laufwerk. Sie können jedoch über eine Vernetzung eine Verbindung zu einem anderen Rechner herstellen, der ein CD-ROM-Laufwerk besitzt bzw. auf dessen Festplatte die CD als Kopie abgelegt werden kann. Zusätzlich ist es notwendig, von den CD-ROMs die Dateien `.S.u.S.E-disk*` auf die Festplatte zu kopieren; in Kurzform geht dies etwa so:

```
erde:~ #  cp /cdrom/.S* /emil
erde:~ #  cp -a /cdrom/suse /emil
```

Dieser „andere“ Rechner muss das Verzeichnis natürlich in geeigneter Weise „exportieren“!

Tipp

Alternativ ist es auch ausreichend, dass Sie auf dem entfernten Rechner das Rettungssystem starten und die CD 1 direkt exportieren.

Tipp

Schritt für Schritt. . .

1. Beginnen Sie die Installation des Clients wie in Abschnitt *Textbasierte Installation mit YaST2* auf Seite 8 ff. beschrieben.

2. Führen Sie die Installation gemäß Abschnitt *Die Grundlage: linuxrc* auf Seite 9 fort, aber beachten Sie bitte folgende Punkte:

   - Laden Sie bei den 'Kernel-Modulen' die 'Netzwerktreiber' und wählen Sie dort den passenden aus; dies ist auch notwendig, wenn Sie per PLIP installieren wollen (in diesem Fall wird die Modul-Diskette angefordert).
   - Geben Sie 'Netzwerk (NFS)' an wenn linuxrc nach dem 'Quellmedium' fragt und führen Sie die menügesteuerte Netzkonfiguration durch. Alternativ können Sie auch per FTP oder SMB installieren.

3. Beenden Sie die Installation wie in [SuS02a], Kapitel *Installation* beschrieben.

Mögliche Probleme

- Die Installation bricht ab, bevor sie überhaupt erst richtig begonnen hat: Das Installationsverzeichnis des „anderen“ Rechners wurde nicht mit `exec`-Rechten exportiert. Holen Sie das bitte nach.

- Der Server erkennt den Rechner nicht, auf dem SuSE Linux installiert werden soll. Tragen Sie den Namen und die IP-Adresse des neu zu installierenden Rechners in der `/etc/hosts` des Servers ein.

Tipps und Tricks

Booten von Diskette (SYSLINUX)

Die „Bootdisk“ kann immer dann zum Einsatz kommen, wenn besondere Anforderungen zum Zeitpunkt der Installation vorliegen (z. B. CD-ROM-Laufwerk nicht verfügbar). Zum Erstellen der Bootdisk vgl. *Bootdiskette unter DOS erstellen* auf der nächsten Seite bzw. *Bootdiskette unter einem unix-artigen System erstellen* auf Seite 22.

Der Bootvorgang wird von dem Bootloader SYSLINUX (Paket `syslinux`) eingeleitet. SYSLINUX ist so konfiguriert, dass in geringem Umfang eine Hardwareerkennung beim Booten durchgeführt wird; im Wesentlichen handelt es sich um die folgenden Schritte:

- Nachschauen, ob das BIOS einen Framebuffer gemäß VESA 2.0 unterstützt und den Kernel entsprechend booten.
- Monitordaten (DDC-Info) auslesen.
- Den 1. Block von der 1. Festplatte („MBR“) lesen, um später bei der LILO-Konfiguration die Zuordnung von BIOS-ID zu Linux-Gerätenamen (engl. *Devices*) hinzubekommen. Dabei wird versucht, den Block über die lba32-Funktionen des BIOS zu lesen, um zu sehen, ob das BIOS diese Funktionen unterstützt.

Tipp

Wenn beim Start von SYSLINUX (Umschalt) bzw. (Shift) gedrückt ist, werden all diese Schritte übersprungen.

Für die Fehlersuche: Man kann in `syslinux.cfg` die Zeile `verbose 1` einfügen; dann teilt der Bootloader mit, welche Aktion jeweils an der Reihe ist.

Tipp

Mögliche Probleme

- Falls der Rechner nicht von Diskette booten will, müssen Sie zuvor möglicherweise die Bootreihenfolge im BIOS des Rechners auf `A,C` umstellen.

CD 2 zum Booten verwenden

Zusätzlich zur CD 1 ist auch die zweite CD bootfähig. Während jedoch auf der CD 1 ein 2,88 MB großes Bootimage verwendet wird, kommt bei der zweiten CD ein traditionelles Image von 1,44 MB Größe zum Einsatz.

Verwenden Sie die CD 2 immer dann, wenn Sie genau wissen, dass Sie von CD booten können, es jedoch mit CD 1 nicht funktioniert („Fallback"-Lösung). Es ist leider so, dass nicht jedes BIOS die großen Images richtig erkennt.

Bootdiskette unter DOS erstellen

Voraussetzung

Sie brauchen eine formatierte 3.5-Zoll-HD-Diskette und ein 3.5-Zoll-Disketten-Laufwerk, das auch bootfähig sein muss.

Zusatzinfo

Auf der CD 1 im Verzeichnis `boot` sind einige Diskettenabbilder (Images) enthalten. Solch ein Image kann mit geeigneten Hilfsprogrammen auf eine Diskette kopiert werden, die Diskette nennt sich dann Bootdiskette. Diese Diskettenimages beinhalten außerdem noch den „Loader" Syslinux und das Programm linuxrc; Syslinux erlaubt es, während des Bootvorganges den gewünschten Kernel auszuwählen und bei Bedarf Parameter über die verwendete Hardware zu übergeben. – Das Programm linuxrc unterstützt Sie beim Laden der Kernelmodule speziell für Ihre Hardware und startet schließlich die Installation.

Vorgehen

Es kommt das DOS-Programm rawrite.exe (CD 1, Verzeichnis `\dosutils\rawrite`) zum Erstellen der SuSE Boot- und Modul-Disketten zum Einsatz. Sie benötigen dazu einen Rechner mit einem DOS (z. B. FreeDOS) oder mit Windows.

Im Folgenden werden die Schritte beschrieben, falls Sie mit Windows arbeiten:

1. Legen Sie die CD 1 von SuSE Linux ein.
2. Öffnen Sie ein DOS-Fenster (im Startmenü unter 'Programme' → 'MS-DOS-Eingabeaufforderung').

3. Starten Sie das Programm rawrite.exe mit der richtigen Pfadangabe für das CD-Laufwerk. Im folgenden Beispiel befinden Sie sich auf der Festplatte `C:` im Verzeichnis `Windows` und Ihr CD-Laufwerk hat den Buchstaben `D:`

   ```
   C:\Windows> d:\dosutils\rawrite\rawrite
   ```

4. Nach dem Start fragt das Programm nach Quelle (engl. *source*) und Ziel (engl. *destination*) der zu kopierenden Datei. Das ist in diesem Beispiel die zum CD-Satz gehörige Bootdiskette, deren Image sich auf CD 1 unter `\disks` befindet. Der Dateiname heißt einfach `bootdisk`. Vergessen Sie auch hier nicht die Pfadangabe für Ihr CD-Laufwerk!

   ```
   C:\Windows> d:\dosutils\rawrite\rawrite
   RaWrite 1.2 - Write disk file to raw floppy diskette
   Enter source file name: d:\disks\bootdisk
   Enter destination drive: a:
   ```

Sobald Sie das Ziellaufwerk `a:` eingegeben haben, fordert Sie rawrite auf, eine formatierte Diskette einzulegen und auf Enter zu drücken. Im weiteren Verlauf wird dann der Fortschritt der Kopieraktion angezeigt. Abbruch ist mit der Tastenkombination Ctrl-c möglich.

Auf diese Art und Weise können Sie auch die anderen Diskettenimages `modules1` und `modules2` erstellen. Diese werden benötigt, wenn Sie SCSI-Geräte oder eine Netzwerkkarte haben und diese während der Installation bereits ansprechen wollen. Bei Problemen kann als Fallback das Image `i386` eingesetzt werden.

Bootdiskette unter einem unix-artigen System erstellen

Voraussetzung

Sie können auf ein unix-artiges oder ein Linux-System mit einem funktionstüchtigen CD-ROM-Laufwerk zurückgreifen. Sie brauchen eine geprüfte Diskette (formatiert).

Gehen Sie so vor, um Bootdisketten zu erstellen:

1. Falls Sie die Disketten noch formatieren müssen:

   ```
   erde:~ #  fdformat /dev/fd0u1440
   ```

2. Mounten Sie die CD 1; z. B. nach `/media/cdrom`:

```
erde:~ #  mount -tiso9660 /dev/cdrom /media/cdrom
```

3. Wechseln Sie in das Verzeichnis `disks` auf der CD:

   ```
   erde:~ #  cd /media/cdrom/boot
   ```

4. Erstellen Sie die Bootdiskette mit

   ```
   erde:~ #  dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
   ```

   In der `LIESMICH`- bzw. der `README`-Datei im `disks`-Verzeichnis erfahren Sie, welcher Kernel was kann; diese Dateien können Sie mit `more` oder `less` lesen.

Auf diese Art und Weise können Sie auch die anderen Diskettenimages `modules1` und `modules2` erstellen. Diese werden benötigt, wenn Sie SCSI-Geräte oder eine Netzwerkkarte haben und diese während der Installation bereits ansprechen wollen. Bei Problemen kann das Image `i386` eingesetzt werden.

Etwas komplexer wird die Angelegenheit, wenn Sie z. B. einen selbst-kompilierten Kernel während der Installation verwenden wollen; schreiben Sie in diesem Fall zunächst das Standard-Image (`bootdisk`) auf die Diskette und überschreiben Sie dann den eigentlichen Kernel (`linux`) mit dem eigenen Kernel (vgl. Abschnitt *Übersetzen des Kernels* auf Seite 192):

```
erde:~ #  dd if=/media/cdrom/boot/bootdisk of=/dev/fd0 bs=8k
erde:~ #  mount -t msdos /dev/fd0 /mnt
erde:~ #  cp /usr/src/linux/arch/i386/boot/vmlinuz /mnt/linux
erde:~ #  umount /mnt
```

Unterstützt Linux mein CD-ROM-Laufwerk?

Generell kann man sagen, dass die meisten CD-ROM-Laufwerke unterstützt werden.

- Bei ATAPI-Laufwerken sollte es keine Probleme geben.
- Bei SCSI-CD-ROM-Laufwerken kommt es nur darauf an, ob der SCSI--Controller unterstützt wird, an dem das CD-ROM-Laufwerk angeschlossen ist – in der Komponenten-Datenbank CDB unter `http://cdb.suse.de/` sind die unterstützten SCSI-Controller aufgeführt. Wenn Ihr SCSI-Controller nicht unterstützt wird und am Controller auch die Festplatte hängt, haben Sie sowieso ein Problem . . .

- Auch viele herstellerspezifische CD-ROM-Laufwerke funktionieren mit Linux. In dieser Gruppe kann es gleichwohl zu Problemen kommen. Falls Ihr Laufwerk nicht explizit erwähnt ist, können Sie es immer noch mit einem ähnlichen Typ des gleichen Herstellers versuchen.
- Mittlerweile sind CD-ROM-Laufwerke am Parallel-Port recht verbreitet. Leider sind diese in keiner Weise standardisiert, sodass es regelmäßig zu Problemen kommt. SuSE Linux enthält eine ganze Reihe verschiedener Alpha-Treiber für einige Laufwerke. Wenn keiner dieser Treiber funktioniert, bleibt nur der Umweg über die DOS-Partition. Beachten Sie, dass einige der Laufwerke, die von Linux unterstützt werden, nur dann angesprochen werden können, wenn sie von ihrem DOS-Treiber initialisiert worden sind und danach nur ein Warmstart ausgeführt wurde.

ATAPI-CD-ROM bleibt beim Lesen hängen

Wenn das ATAPI-CD-ROM-Laufwerk nicht erkannt wird oder es beim Lesen hängen bleibt, ist häufig die Hardware nicht korrekt eingerichtet. Normalerweise sollten die einzelnen Geräte am (E)IDE-Bus fortlaufend angeschlossen sein, d. h. das erste Gerät ist Master am ersten Controller, das zweite Slave. Das dritte Gerät schließlich ist Master am zweiten Controller und das vierte dort wieder Slave.

Oft befindet sich in einem Rechner neben der Festplatte nur das CD-ROM-Laufwerk, das als Master am zweiten Controller hängt. Linux kommt in manchen Fällen mit dieser „Lücke“ nicht selbstständig zurecht. Meistens kann dem Kernel durch Angabe eines entsprechenden Parameters aber auf die Sprünge geholfen werden (`hdc=cdrom`).

Gelegentlich ist ein Laufwerk nur falsch „gejumpert“; das heißt, es ist als Slave konfiguriert, obwohl es als Master am zweiten Controller angeschlossen ist oder umgekehrt. Im Zweifelsfall sollten diese Einstellungen überprüft und gegebenenfalls korrigiert werden.

Außerdem gibt es noch eine Reihe fehlerhafter EIDE-Chipsätze. Diese sind mittlerweile zum größten Teil bekannt; der Kernel enthält Code, um derartige Probleme zu umgehen. Für diese Fälle existiert ein spezieller Kernel (vgl. das `README` in `/disks` der Installations-CD-ROM).

Sollte das Booten nicht auf Anhieb funktionieren, so versuchen Sie bitte die nachfolgenden Kernelparameter:

hd⟨*x*⟩=cdrom ⟨*x*⟩ steht hier für `a`, `b`, `c`, `d` etc. und ist folgendermaßen zu lesen:

- `a` – Master am 1. IDE-Controller
- `b` – Slave am 1. IDE-Controller
- `c` – Master am 2. IDE-Controller
- ...

Beispiel für ⟨*einzugebender Parameter*⟩: `hdb=cdrom`

Mit diesem Parameter geben Sie dem Kernel das CD-ROM-Laufwerk an, falls er es nicht selbst findet und Sie ein ATAPI-CD-ROM-Laufwerk haben.

`ide`⟨*x*⟩`=noautotune` ⟨*x*⟩ steht für `0`, `1`, `2`, `3` etc. und ist folgendermaßen zu lesen:

- `0` – 1. IDE-Controller
- `1` – 2. IDE-Controller
- ...

Beispiel für ⟨*einzugebender Parameter*⟩: `ide0=noautotune`

Dieser Parameter hilft in der Regel bei (E)IDE-Festplatten.

CD-ROM-Laufwerke am Parallelport

Alle verfügbaren Treiber werden während der Installationsphase von linuxrc zur Auswahl angeboten. Im Regelfall sind keine Besonderheiten zu beachten.

Leider werden viele Laufwerke (z. B. von Freecom) noch nicht unterstützt. Bisweilen können Laufwerke nicht benutzt werden, die laut Aufschrift typenidentisch sein sollten; die Hersteller haben offensichtlich Interna geändert, ohne diese Änderungen durch eine neue Typenbezeichnung kenntlich zu machen...

Einige der Laufwerke müssen vom zugehörigen DOS-Treiber initialisiert worden sein, bevor der Linux-Kernel sie erkennt:

1. Booten Sie DOS und lassen Sie den CD-ROM-Treiber laden.
2. Legen Sie die Linux-Bootdiskette ein.
3. Führen Sie einen Warmstart durch.

Bei nicht unterstützten Laufwerken muss nach wie vor mit Umweg über eine DOS-Partition installiert werden (vgl. Abschnitt *Besondere Installationen* auf Seite 18).

Zum Stand der Parallelport-Programmierung unter Linux vgl. `http://www.torque.net/linux-pp.html`.

loadlin fehlt Speicher, um den Kernel zu laden

Sie haben nicht genügend freien Speicher unterhalb 640 KB. Versuchen Sie, aus den Startdateien des Systems (`config.sys`, `autoexec.bat`) einige Treiber zu entfernen oder in den hohen Speicherbereich zu laden.

Falls Sie unter Windows 95/98 komprimierte Laufwerke haben und das Hochladen des Treibers nicht hilft, müssen Sie die komprimierten Laufwerke dekomprimieren.

loadlin funktioniert nicht

Falls es mit loadlin irgendwelche Probleme gibt, können Sie `loadlin` mit den Optionen `-v`, `-t` oder `-d` aufrufen. Am Besten lassen Sie mit

```
C:\> loadlin -d debug.out ⟨weitere Parameter⟩
```

die Debug-Informationen in die Datei `debug.out` schreiben; diese Datei können Sie dem SuSE-Support schicken. Für ⟨*weitere Parameter*⟩ müssen Sie Ihre eigenen System-Gegebenheiten einsetzen (vgl. Abschnitt *Notwendige Dateien für loadlin* auf Seite 112).

Partitionieren für Fortgeschrittene

Im Kapitel zur Standardinstallation (siehe [SuS02b]) wird auf Möglichkeiten der Partitionierung des Systems eingegangen. Dieser Abschnitt soll nun detaillierte Informationen bereitstellen, mit denen Sie sich ein für Ihre Zwecke optimales Partitionierungsschema anlegen können. Dieser Abschnitt ist insbesondere für diejenigen interessant, die ihr System optimal konfigurieren möchten – sowohl in puncto Sicherheit, als auch was Geschwindigkeit betrifft – und die dafür bereit sind, u. U. das bestehende System komplett neu aufzusetzen. Tabula rasa, wenn man so will.

Es ist unbedingt notwendig, ein grundlegendes Verständnis der Funktionsweise eines UNIX-Dateisystemes zu haben. Die Begriffe Mountpoint, sowie physikalische, erweiterte und logische Partition sollten keine Fremdwörter sein.

Zunächst sollte erwähnt werden, dass es nicht den *einen* goldenen Weg für alle gibt, sondern viele goldene Wege für jeden. Keine Sorge, Sie werden in diesem Abschnitt auch konkrete Zahlen als Anhaltspunkt lesen.

Stellen Sie als ersten Schritt folgende Informationen zusammen:

- Was ist das Einsatzgebiet dieses Rechners (Fileserver, Application-Server, Compute-Server, Einzelplatzrechner)?
- Wie viele Leute werden an diesem Rechner arbeiten (simultane Logins)?
- Wie viele Festplatten hat der Rechner, wie groß sind diese und welches System haben Sie (EIDE-, SCSI- oder RAID-Controller)?

Die Größe der Swap-Partition

Oft werden Sie noch lesen: „Mindestens doppelt so viel Swap wie Hauptspeicher". Diese Formulierung stammt noch aus der Zeit, in der 8 MB RAM im Rechner nicht wenig war. Diese Zeiten sind vorbei. Wer sich heute einen neuen Rechner mit weniger als 64 MB Speicher kauft, wurde nicht gut beraten. Kommen wir noch einmal zur obigen Aussage zurück. Ziel war es, dass der Rechner über ungefähr 30 bis 40 MB virtuellen Speicher verfügt.

Mit modernen Speicher hungrigen Applikationen müssen auch diese Werte nach oben hin korrigiert werden. Im Normalfall sollten 128 MB virtueller Speicher genügen, aber hier sollte man nicht geizen. Compiliert man unter X seinen Kernel und will sich mit Netscape die Hilfeseiten ansehen, während noch irgendwo Emacs läuft, hat man mit 128 MB virtuellem Speicher nicht mehr viele Reserven.

Daher ist man als durchschnittlicher User für absehbare Zeit mit 256 MB virtuellem Speicher auf der sicheren Seite. Was Sie auf keinen Fall machen sollten: überhaupt keinen Swap-Speicher anlegen. Selbst auf einem Rechner mit 256 MB RAM sollte noch ein Swap-Bereich vorhanden sein. Die Gründe hierfür werden unter Abschnitt *Plattendurchsatz und die Größe des Hauptspeichers* auf Seite 31 deutlich.

Sie lassen umfangreiche Simulationen mit einem Speicherbedarf (!) von mehreren Gigabyte berechnen. Wenn Sie Bedenken haben sollten, ob Linux für Ihre Anwendung genügend Reserven bietet, lesen Sie Abschnitt *Einsatz als Compute-Server* auf Seite 29 (Einsatzgebiet Compute-Server).

Einsatzgebiet des Rechners

Einsatz als Einzelrechner

Der häufigste Anwendungsfall für einen Linux-Rechner ist der Einsatz als Einzelrechner. Damit Sie sich an konkreten Werten orientieren können, haben wir ein paar Beispielkonfigurationen zusammengestellt, die Sie je nach Bedarf

Installation	benötigter Plattenplatz
sehr klein	180 MB bis 400 MB
klein	400 MB bis 800 MB
mittel	800 MB bis 4 GB
groß	4 GB bis 8 GB

Tabelle 1.1: *Beispiele für Größen von Installationen*

bei sich zu Hause oder in der Firma übernehmen können. In Tabelle 1.1 sehen Sie einen kleinen Überblick der verschiedenen Installationsvolumina für ein Linux-System.

Natürlich erhöhen sich die Werte entsprechend, wenn Sie über das System hinausgehende, zusätzliche Datensätze sichern wollen.

Beispiel: Standard-Arbeitsplatzrechner (sehr klein)

Sie haben eine ca. 500 MB große Festplatte übrig und möchten auf diese Linux installieren: eine 64 MB große Swap-Partition und den Rest für `/` (Root-Partition).

Beispiel: Standard-Arbeitsplatzrechner (Durchschnitt)

Sie haben 1,2 GB für Linux frei. Kleine Boot-Partition `/boot` (5-10 MB bzw. 1 Zylinder), 128 MB für Swap, 800 MB für `/` und den Rest für eine separate `/home`-Partition.

Beispiel: Standard-Arbeitsplatzrechner (Luxus)

Falls Ihnen 1,2 GB oder mehr auf mehreren Platten zur Verfügung stehen, gibt es keine pauschale Partitionierung. Lesen Sie hierzu bitte Abschnitt *Optimierungsmöglichkeiten* auf der nächsten Seite.

Einsatz als Fileserver

Hier kommt es *wirklich* auf Festplattenperformance an. SCSI-Geräten sollte unbedingt der Vorzug gegeben werden. Achten Sie auch auf Leistungsfähigkeit der Platten und des verwendeten Controllers.

Ein Fileserver bietet die Möglichkeit, Daten zentral zu halten. Hierbei kann es sich um Benutzerverzeichnisse, eine Datenbank oder sonstige Archive handeln. Der Vorteil ist eine wesentlich einfachere Administration.

Falls der Fileserver ein größeres Netz bedienen soll (ab 20 Usern), wird die Optimierung des Plattenzugriffs essentiell.

Angenommen, Sie möchten einen Linux-Fileserver aufbauen, der 25 Benutzern Heimatverzeichnisse (Home) zur Verfügung stellen soll. Sie wissen, jeder Benutzer wird maximal 100-150 MB für seine persönlichen Daten in Anspruch nehmen. Falls nicht jeder dieser Benutzer stets in seinem Home kompiliert, reicht hierfür eine 4-GB-Platte, welche einfach unter `/home` gemountet wird.

Haben Sie 50 Benutzer, so wäre rein rechnerisch eine 8-GB-Platte notwendig. Besser ist es in diesem Fall jedoch, `/home` auf zwei 4-GB-Platten aufzuteilen, da sich diese dann die Last (und Zugriffszeit!) teilen.

Tipp

Den Cache eines Webbrowsers sollten die Benutzer unbedingt auf lokalen Festplatten halten!

Tipp

Einsatz als Compute-Server

Ein Compute-Server ist in der Regel ein leistungsstarker Rechner, der berechnungsintensive Aufgaben im Netz übernimmt. Solch eine Maschine verfügt typischerweise über einen etwas größeren Hauptspeicher (ab 512 MB RAM). Der einzige Punkt, an dem für einen schnellen Plattendurchsatz gesorgt werden muss, sind etwaige Swap-Partitionen. Auch hier gilt: mehrere Swap-Partitionen auf mehrere Platten verteilen.

Optimierungsmöglichkeiten

Die Platten sind zumeist der begrenzende Faktor. Um diesen Flaschenhals zu umgehen, gibt es drei Möglichkeiten, die am Besten zusammen eingesetzt werden sollten:

- Verteilen Sie die Last gleichmäßig auf mehrere Platten.
- Setzen Sie ein optimiertes Dateisystem ein (z. B. `reiserfs`).
- Statten Sie den Fileserver mit genügend Speicher aus (256 MB Minimum).

Parallelisierung durch mehrere Platten

Die erstgenannte Methode bedarf einer tiefer gehenden Erklärung. Die Gesamtzeit, die vergeht, bis angeforderte Daten bereitgestellt werden, setzt sich (in etwa) aus folgenden Teilen zusammen:

1. Zeit, bis die Anforderung beim Plattencontroller ist.
2. Zeit, bis der Plattencontroller diese Anforderung an die Festplatte schickt.
3. Zeit, bis die Festplatte ihren Kopf positioniert.
4. Zeit, bis sich das Medium zum richtigen Sektor gedreht hat.
5. Zeit für die Übertragung.

Punkt 1 ist abhängig von der Anbindung über das Netzwerk und muss dort geregelt werden. Dies wollen wir hier nicht weiter betrachten. Punkt 2 ist eine relativ vernachlässigbare Zeit, die vom Plattencontroller selbst abhängt. Punkt 3 ist eigentlich der Hauptbrocken. Gemessen wird die Positionierung in ms. Verglichen mit den in ns gemessenen Zugriffszeiten im Hauptspeicher ist das ein Faktor von 1 Million! Punkt 4 ist von der Drehzahl der Platte abhängig. Punkt 5 von der Drehzahl und der Anzahl der Köpfe, ebenso wie von der aktuellen Position des Kopfes (innen oder außen).

Für die optimale Performance sollte man also bei Punkt 3 angreifen. Hier kommt bei SCSI-Geräten das Feature „disconnect“ ins Spiel. Mit diesem Feature passiert in etwa folgendes:

Der Controller sendet an das angeschlossene Gerät (in diesem Fall die Festplatte) den Befehl „Gehe zu Track x, Sektor y“. Nun muss sich die träge Mechanik der Platte in Bewegung setzen. Wenn die Platte intelligent ist (also disconnect beherrscht) und der Treiber für den Controller dieses Feature auch beherrscht, schickt der Controller der Platte unmittelbar daraufhin einen disconnect-Befehl und die Platte trennt sich vom SCSI-Bus ab. Ab jetzt können andere SCSI-Geräte ihre Transfers erledigen. Nach einer Weile (je nach Strategie bzw. Last auf dem SCSI-Bus) wird wieder die Verbindung zur Platte aktiviert. Idealerweise hat diese bereits den geforderten Track erreicht.

In einem Multitasking-Multiuser Betriebssystem wie Linux kann man hier natürlich gut optimieren. Sehen wir uns einen Ausschnitt einer Ausgabe des Befehls `df` an (vgl. Ausgabe 1).

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda5             1.8G  1.6G  201M  89% /
```

```
/dev/sda1                 23M  3.9M   17M  18% /boot
/dev/sdb1                2.9G  2.1G  677M  76% /usr
/dev/sdc1                1.9G  958M  941M  51% /usr/lib
shmfs                    185M     0  184M   0% /dev/shm
```

***Ausgabe 1:** Beispielausgabe df-Befehl*

Was bringt uns diese Parallelisierung? Angenommen wir geben in /usr/src ein:

```
root@erde:/usr/src/ >  tar xzf package.tar.gz -C /usr/lib
```

Das soll also package.tar.gz nach /usr/lib/package installieren. Hierzu werden von der Shell tar und gzip aufgerufen (befinden sich in /bin und somit auf /dev/sda), dann wird package.tar.gz von /usr/src gelesen (befindet sich auf /dev/sdb). Als Letztes werden die extrahierten Daten nach /usr/lib geschrieben (liegt unter /dev/sdc). Sowohl Positionierung, als auch Lesen/Schreiben der platteninternen Puffer können nun quasiparallel ausgeführt werden.

Das ist ein Beispiel von vielen. Als Faustregel gilt, dass bei Vorhandensein entsprechend vieler (gleich schneller) Platten /usr und /usr/lib auf verschiedenen Platten lagern sollten. Hierbei sollte /usr/lib ca. 70 % der Kapazität von /usr haben. Das Rootverzeichnis / sollte sich bei der Verlagerung auf zwei Platten wegen der Zugriffshäufigkeit auf der Platte mit /usr/lib befinden.

Ab einer gewissen Menge an SCSI-Platten (ca. 4 bis 5) sollte man sich jedoch ernsthaft mit einer RAID-Lösung in Software oder gleich besser mit der Anschaffung eines RAID-Controllers beschäftigen. Dadurch werden dann Operationen auf den Platten nicht nur quasiparallel, sondern echt parallel ausgeführt. Fehlertoleranz ist ein weiteres angenehmes Nebenprodukt.

Plattendurchsatz und die Größe des Hauptspeichers

Wir weisen an vielen Stellen darauf hin, dass die Größe des Hauptspeichers unter Linux oft wichtiger ist als die Geschwindigkeit des Prozessors. Ein Grund – wenn nicht sogar der Hauptgrund – ist die Eigenschaft von Linux, dynamische Puffer mit Festplattendaten anzulegen. Hierbei arbeitet Linux mit allerlei Tricks wie „read ahead“ (holt vorsorglich Sektoren im Voraus) und „delayed write“ (spart sich Schreibzugriffe, um sie dann in einem Aufwasch auszuführen). Letzteres ist der Grund, warum man einen Linux-Rechner nicht einfach ausschalten darf. Beide Punkte sind dafür verantwortlich, dass sich der Hauptspeicher mit der Zeit immer scheinbar füllt und dass Linux so schnell ist; vgl. auch Abschnitt *Der Befehl free* auf Seite 201.

Update des Systems und Paketverwaltung

SuSE Linux bietet die Möglichkeit, ein bestehendes System ohne Neuinstallation zu aktualisieren. Dabei muss unterschieden werden zwischen der *Aktualisierung einzelner Softwarepakete* und einem *Update des gesamten Systems*.

Einzelne Pakete können auch von Hand mit dem Paketmanager rpm installiert werden.

SuSE Linux aktualisieren 34
Softwareänderungen von Version zu Version 39
RPM – Der Paket-Manager der Distribution 48

SuSE Linux aktualisieren

Es ist ein bekanntes Phänomen, dass Software von Version zu Version „wächst“. Deshalb empfiehlt es sich *vor* dem Update mit `df` nachzuschauen, wie sehr die einzelnen Partitionen bereits ausgelastet sind. Wenn Sie den Eindruck haben, es könnte knapp werden, dann führen Sie bitte vor dem Update ein Datenbackup durch und partitionieren Sie das System neu. Es kann kein genereller Tipp gegeben werden, wie viel Platz jeweils im Einzelnen benötigt wird – der Platzbedarf ist abhängig von der Art der bestehenden Partitionierung, von der ausgewählten Software und von der Versionsnummer des bestehenden Systems auf das vorliegende SuSE Linux 8.1.

Hinweis

Es ist empfehlenswert, auf der CD die Datei `LIESMICH` (engl. *`README`*) bzw. unter DOS/Windows die Datei `LIESMICH.DOS` (engl. *`README.DOS`*) zu lesen; dort notieren wir zusätzliche Änderungen, die *nach* der Drucklegung des Handbuchs erfolgt sind!

Hinweis

Vorbereitungen

Vor Beginn eines Updates sollten sicherheitshalber die alten Konfigurationsdateien auf ein separates Medium (Streamer, Wechselplatte, Disketten, ZIP-Laufwerk) kopiert werden. In erster Linie handelt es sich um die Dateien, die in `/etc` gespeichert sind; weiterhin sind die Konfigurationsdateien unter `/var/lib` zu kontrollieren. Zudem kann es nichts schaden, die aktuellen Benutzerdaten unter `/home` (die `HOME`-Verzeichnisse) auf ein Backup-Medium zu schreiben. Das Sichern der Daten ist als Systemadministrator `root` durchzuführen; nur `root` hat die Rechte, alle lokalen Dateien zu lesen.
Bevor Sie den Update-Vorgang einleiten, notieren Sie sich die Rootpartition; mit dem Kommando

```
erde:~ #  df /
```

können Sie den Gerätenamen der Rootpartition herausfinden; in dem Fall der Ausgabe 2 ist `/dev/hda7` die zu notierende Root-Partition.

```
Dateisystem          Größe Benut  Verf Ben% montiert auf
/dev/hda1             1.9G  189M  1.7G  10% /dos
/dev/hda7             3.0G  1.1G  1.7G  38% /
/dev/hda5              15M  2.4M   12M  17% /boot
```

Ausgabe 2: *Überblick mit df -h*

Denn die Ausgabe zeigt, dass die Partition /dev/hda7 unter / in das Dateisystem eingehängt („gemountet“) ist.

Mögliche Probleme

PostgreSQL Vor einem PostgreSQL-Update (Paket postgres) empfiehlt es sich in der Regel, die Datenbanken zu „dumpen“; vgl. Manual-Page von pg_dump (man pg_dump). Dies ist natürlich nur dann erforderlich, wenn Sie PostgreSQL vor dem Update tatsächlich *benutzt* haben.

Promise-Controller Die Festplatten-Controller der Firma Promise finden sich inzwischen auf hochwertigen Mainboards in verschiedenen Rechnern. Manchmal als reine IDE-Controller (für UDMA 100), manchmal als IDE-RAID-Controller. Seit SuSE Linux 8.0 werden diese Controller direkt vom Kernel unterstützt und als normale Controller für IDE-Festplatten behandelt. Erst das zusätzlich Kernel-Modul pdcraid ermöglicht die RAID-Funktionalität.

In manchen Fällen kann es beim Update passieren, dass Festplatten am Promise-Controller vor den Festplatten am normalen IDE-Controller erkannt werden. Das System wird dann nach einem Kernel-Update nicht mehr booten und sich typischerweise mit "Kernel panic: VFS: unable to mount root fs" verabschieden. In diesem Fall muss beim Booten der Kernel-Parameter ide=reverse angegeben werden, um die Reihenfolge der Plattenerkennung umzudrehen; vgl. Abschnitt *Der Startbildschirm* auf Seite 8. Dieser Parameter muss für dauerhafte Verwendung mit YaST2 in die Bootkonfiguration eingetragen werden; vgl. das Kapitel *YaST2, Boot-Modus* im Handbuch [SuS02a].

Achtung

Nur die im BIOS eingeschalteten Controller werden gefunden. Insbesondere hat das nachträgliche Ein- oder Aussschalten von Controllern im BIOS direkte Auswirkungen auf die Devicenamen. Bei unbedachtem Vorgehen ist unter Umständen das Booten nicht mehr möglich!

Achtung

Technische Erklärung
Die Reihenfolge der Controller hängt vom Mainboard ab, jeder Hersteller hat seine eigene Strategie, Zusatzcontroller zu verdrahten. Mit dem Befehl lspci wird diese Reihenfolge sichtbar. Wenn der Promise-Controller vor dem normalen IDE-Controller aufgeführt wird, ist der Kernel-Parameter ide=reverse nach einem Update notwendig. Mit

dem alten Kernel (ohne direkte Promise Unterstützung) wurde der Controller ignoriert und der normale IDE-Controller zuerst erkannt. Die erste Platte war dann `/dev/hda`. Mit dem neuen Kernel wird der Promise-Controller direkt gefunden und seine (bis zu vier) Platten als `/dev/hda`, `/dev/hdb`, `/dev/hdc` und `/dev/hdd` gemeldet. Die bisherige `/dev/hda`-Platte wird plötzlich zu `/dev/hde` und daher beim Bootvorgang nicht mehr gefunden.

Update mit YaST2

Nach den in Abschnitt *Vorbereitungen* auf Seite 34 genannten Vorarbeiten booten Sie.

Starten Sie das System wie zur Installation und wählen Sie dann in YaST2–nach Bestätigung der Sprache – 'Update des bestehenden Systems'. YaST2 wird ermitteln, welche Rootpartitionen vorhanden und welche Pakete zu aktualisieren sind. Zudem gibt es die Möglichkeit, die System durch neue wichtige Softwarekomponenten zu bereichern.

die werden

Manuell gesteuertes Update

Das Basissystem erneuern

Da beim Aktualisieren des Grundsystems die zentralen Bestandteile des Systems (wie z. B. Bibliotheken) ausgetauscht werden müssen, kann diese Aufgabe nicht im normalen Betrieb, d. h. aus dem bereits laufenden Linuxsystem heraus, erledigt werden.

Sie müssen also die Update-Umgebung starten. Dies geschieht im Normalfall mit der CD bzw. DVD oder mit der selbsterstellten Diskette zum Booten („Bootdisk"). Wenn Sie manuelle Eingriffe während des Updates vornehmen oder das gesamte Update mit der „ncurses-ui" von YaST2 (Textmodus) durchführen wollen, sind im Wesentlichen die Schritte notwendig, die bereits in Abschnitt *Textbasierte Installation mit YaST2* auf Seite 8 ff. ausführlich beschrieben sind:

1. Direkt im Anschluss an das Booten des Kernels von der „Bootdisk" oder der CD bzw. DVD wird automatisch linuxrc gestartet.

2. Im linuxrc sind im Hauptmenü unter dem Menüpunkt 'Einstellungen' Sprache und Tastatur festzulegen und jeweils mit 'Ok' zu bestätigen.

3. Über den Menüpunkt 'Kernel-Module' müssen ggf. die notwendigen Hardware- und SoftwareTreiber geladen werden; zum genauen Vorgehen vgl. Abschnitt *Die Grundlage: linuxrc* auf Seite 9 und die linuxrc-Beschreibung auf Seite 209.

4. Es kann über die Menüpunkte 'Installation / System starten' → 'Installation/Update starten' zur Auswahl des Quellmediums übergegangen werden (vgl. auf Seite 211).

5. Von linuxrc wird die Installationsumgebung geladen und es wird YaST2 gestartet.

Im Eingangsmenü von YaST wählen Sie – nach Kontrolle der Sprache und Überprüfung der Hardware durch YaST2– den Punkt 'Update des bestehenden Systems'.

Im Anschluss versucht YaST die Root-Partition herauszufinden und bietet das Ergebnis zur Auswahl bzw. Bestätigung an; in der angezeigten Liste geben Sie Ihre Root-Partition an, wie oben notiert (Beispiel: `/dev/sda3`). So beauftragen Sie YaST, die „alte" `fstab` einzulesen, die sich auf dieser Partition befindet; YaST wird die dort eingetragenen Dateisysteme analysieren und dann mounten.

Danach besteht die Möglichkeit, eine Sicherungskopie der Systemdateien während des Updates erstellen zu lassen.

Entweder kann im folgenden Dialog festgelegt werden, dass nur die bereits installierte Software erneuert wird oder dass dem System wichtige neue Softwarekomponenten hinzugesellt werden („Upgrade-Modus"). Es ist empfehlenswert, die vorgegebene Zusammenstellung zu akzeptieren (z. B. 'Standard-System'). Etwaige Unstimmigkeiten können Sie mit YaST2 beseitigen.

Warndialog: 'Ja', damit das Übertragen der neuen Software von dem Quellmedium auf die Festplatte des Systems geschehen kann.

Überprüfung der RPM-Datenbank.

Anschließend werden zunächst die zentralen Bestandteile des Systems aktualisiert, wobei YaST automatisch Sicherungen von Dateien anlegt, die seit der letzten Installation während des Betriebs verändert wurden; weiterhin werden alte Konfigurationsdateien ggf. mit der Endung `.rpmorig` bzw. `.rpmsave` gesichert (vgl. Abschnitt *Pakete verwalten: Installieren, Updaten und Deinstallieren* auf Seite 50); der Vorgang der Installation bzw. des Updates wird in `/var/adm/inst-log/installation-*` protokolliert und ist jederzeit nachlesbar.

Update des restlichen Systems

Ist das Basissystem aktualisiert, gelangen Sie in einen speziellen Update--Modus von YaST. Dort können Sie nach Ihren Wünschen den Rest des Systems updaten.

Nachdem diese Aufgabe erledigt ist, müssen Sie den Vorgang wie eine Erstinstallation abschließen. Unter anderem sollten Sie einen neuen Kernel auswählen; YaST wird diese Option anbieten.

Tipp

Wenn Sie es gewohnt sind, mit loadlin zu booten, müssen Sie den *neuen* Kernel und eventuell die `initrd` zudem in das `loadlin`-Verzeichnis Ihrer DOS-Partition kopieren!

Tipp

Mögliche Probleme

- Falls sich nach dem Update bestimmte Shell-Umgebungen nicht mehr so verhalten wie gewohnt, konrollieren Sie bitte unbedingt, ob die aktuellen „Punkt"-Dateien im Homeverzeichnis noch zum System passen. Ist dies nicht der Fall, übernehmen Sie bitte die aktuellen Versionen von `/etc/skel`; z. B.:

```
tux@erde:~ >  cp /etc/skel/.profile ~/.profile
```

Aktualisieren einzelner Pakete

Unabhängig von einem Gesamt-Update können Sie jederzeit einzelne Pakete aktualisieren; dabei müssen Sie *selbst* freilich darauf achten, dass das System konsistent bleibt: Update-Empfehlungen finden Sie unter `http://www.suse.de/de/support/download/updates/` aufgelistet.

In der Paketauswahl von YaST (siehe Abschnitt *Software* auf Seite 66 ff.) können Sie nach Herzenslust schalten und walten. Wählen Sie ein Paket zum Update aus, das für den Betrieb des Systems eine zentrale Rolle spielt, werden Sie von YaST gewarnt. Derartige Pakete sollten im speziellen Update-Modus aktualisiert werden. Beispielsweise enthalten etliche Pakete „shared libraries", die möglicherweise zum Zeitpunkt des Updates von laufenden Prozessen verwendet werden. Ein Update im laufenden System würde daher dazu führen, dass diese Programme nicht mehr korrekt funktionieren können.

Softwareänderungen von Version zu Version

In den folgenden Abschnitten wird aufgelistet, welche Details sich von Version zu Version geändert haben. In dieser Übersicht erscheint beispielsweise, ob grundlegende Einstellungen neu vorgenommen oder ob Konfigurationsdateien an andere Stellen verschoben wurden oder ob bekannte Programme erkennbar modifiziert wurden. Es werden nur die Dinge genannt, die den Benutzer bzw. den Administrator bei der täglichen Arbeit unmittelbar berühren. Die Liste ist keineswegs erschöpfend und vollständig. Im Folgenden wird mitunter auf SDB-Artikel verwiesen; die Artikel der SDB (Support Datenbank) sind im Paket `sdb_de` enthalten.

Probleme und Besonderheiten der jeweiligen Version werden bei Bekanntwerden auf dem WWW-Server veröffentlicht; vgl. die unten angegebenen Links. Wichtige Updates einzelner Pakete sind über `http://www.suse.de/de/support/download/updates/` zugänglich.

Von 6.x auf 7.0

Probleme und Besonderheiten:
`file:/usr/share/doc/sdb/de/html/bugs61.html`
`file:/usr/share/doc/sdb/de/html/bugs62.html`
`file:/usr/share/doc/sdb/de/html/bugs63.html`
`file:/usr/share/doc/sdb/de/html/bugs64.html`
`file:/usr/share/doc/sdb/de/html/bugs70.html`

- Es werden unterschiedlich optimierte Kernel zur Installation angeboten; diese Kernel verwenden eine „initrd“ (engl. *Initial Ramdisk*). Beim Erzeugen eines eigenen Kernels ist dieses Merkmal zu beachten; vgl. Abschnitt *Mögliche Schwierigkeit – Selbstcompilierte Kernel* auf Seite 206 und `file:/usr/share/doc/sdb/de/html/adrian_6.3_boot.html`.
- Alle Kernelmodule („Treiber“) sind Bestandteil des jeweils installierten Kernels (Single-, Multiprozessor-Kernel etc.); so wird sichergestellt, dass die passend kompilierten Module installiert sind. Paket `kernmod` bzw. Paket `kernmods` sind nicht mehr notwendig. Die Konfigurationsdateien des installierten Kernels liegen unter `/boot` als `vmlinuz.config-pentium` (Beispiel!), `vmlinuz.autoconf.h` und `vmlinuz.version.h`.
- Die Konfigurationsdatei für die Kernel-Module heißt in Übereinstimmung mit vielen anderen Konfigurationsdateien `/etc/modules.conf` (früher: `/etc/conf.modules`).

- Zu der glibc gehört auch der nscd (engl. *Name Service Cache Daemon*), der über die Datei `/etc/nscd.conf` konfiguriert wird; vgl. Manual-Page von `nscd` (`man 8 nscd`).

- Mit der aktuellen glibc wird der Umstieg auf „Unix98 PTY"-Devices vollzogen. Dies bedingt, dass auch das `devpts`-Dateisystem zu mounten ist; folgender Eintrag in der `/etc/fstab` stellt dies beispielsweise sicher:

```
none    /dev/pts    devpts    gid=5,mode=620    0 0
```

  Vgl. auch die Dokumentation in `/usr/src/linux/Documentation/Changes` bei den Kernelquellen (Paket `kernel-source`).

- PAM (engl. *Pluggable Authentication Modules*): Zusätzlich zu `/etc/login.defs` gibt es nun `/etc/securetty`, `/etc/security/limits.conf` und `/etc/security/pam_env.conf`.

- Gültige *Login-Shells* sind in `/etc/shells` eingetragen; vgl. Manual-Page von `shells` (`man 5 shells`). Wird einem Benutzer `/bin/true` zugeordnet, so kann sich dieser Benutzer nur über das X Window System anmelden; dieser Benutzer bekommt keine Shell. `/bin/false` als „Login-Shell" verhindert jegliche Anmeldung.

- Das X Window System 4.0 unterstützt einige alter Grafikkarte nicht mehr bzw. einige neue Karten noch nicht; vgl. Abschnitt **??** auf Seite ??. Das Setup-Programm wird diesen Umstand bemerken und automatisch auf die weiterhin mitgelieferte Vorgängerversion 3.3.x ausweichen.

- Um die Sicherheit zu erhöhen, ist der XDM nun so voreingestellt, dass XDMCP- oder Chooser-Anfragen *nicht* angenommen werden. Wenn Sie z. B. X-Terminals bedienen wollen, muss in `/etc/X11/xdm/xdm-config` (früher `/var/X11R6/lib/xdm/xdm-config`) die Zeile mit der Option `DisplayManager.requestPort` durch Voranstellen eines Ausrufungszeichens auskommentiert werden; vgl. Manual-Page von `xdm` (`man xdm`):

```
!DisplayManager.requestPort:    0
```

- rpm (vgl. auch Abschnitt *RPM – Der Paket-Manager der Distribution* auf Seite 48) liegt in der Version 3.0 vor. Das Format der RPM-Datenbank hat sich geändert; die Datenbank muss sofort konvertiert werden, wenn rpm installiert ist. Bei einem regulären Update des (Basis-)Systems mit YaST wird die Konvertierung zum richtigen Zeitpunkt im Hintergrund durchgeführt.

- Dem FHS (engl. *Filesystem Hierarchy Standard*) gemäß (vgl. Abschnitt *Filesystem Hierarchy Standard (FHS)* auf Seite 196) ist die architekturunabhängige Dokumentation nun unter `/usr/share/doc` zu finden (früher `/usr/doc`).

- Die Manual-Pages liegen unter `/usr/share/man` und die Info-Seiten liegen unter `/usr/share/info`, wie es der FHS (engl. *Filesystem Hierarchy Standard*) verlangt; vgl. Abschnitt *Filesystem Hierarchy Standard (FHS)* auf Seite 196.

- `makewhatis` (Paket `makewhat`) verwendet nun das Hilfsprogramm `manpath`, um die *Manual-Pages* zu finden. Die Umgebungsvariable `MANPATH` soll in `rc`-Dateien nicht mehr gesetzt werden.

- Eine neuere Version von tar wird mitgeliefert. Das Überschreibverhalten beim Auspacken vorhandener Dateien ist geändert; wenn Sie auf den alten Modus angewiesen sind, verwenden Sie bitte die Option `--overwrite`.

- Unter X ist die Compose-Taste („Multi_key“) über die Tastenkombination ⇑ + Ctrl (rechts) zu erreichen; vgl. Abschnitt *Tastaturbelegung* auf Seite 219.

- Aus Sicherheitsgründen ist *anonymes FTP* nicht mehr automatisch zugelassen. Um bei dem FTP-Daemon `in.ftpd` anonymes FTP zu erlauben, muss in `/etc/pam.d/ftpd` das Kommentarzeichen `'#'` entfernt werden vor der Zeile:

```
auth    sufficient   /lib/security/pam_ftp.so
```

- *Passwort* ändern mit PAM (engl. *Pluggable Authentication Modules*): `pam_unix` kann auch NIS-Passwörter ändern und versteht `md5`-Hashes als Passwort. Vorsicht!

  Außerdem gibt es jetzt ein neues `pam_pwcheck`-Module, welches die Überprüfung neuer Passwörter übernimmt. Der alte Eintrag:

```
password required  /lib/security/pam_unix.so  #strict=false
```

  muss geändert werden in (jeweils nur eine Zeile oder mit \ („Gegenstrich“) am Zeilenende!):

```
password required   /lib/security/pam_pwcheck.so \
                    nullok #use_cracklib
password required   /lib/security/pam_unix.so    \
                    nullok use_first_pass use_authtok
```

Dieser manuelle Eingriff ist nur notwendig, falls rpm beim Update die Konfigurationsdateien nicht selbst ändern darf, da der Systemadministrator eigene Änderungen gemacht hat. Dies gilt übrigens für alle Konfigurationsdateien von PAM unter /etc/pam.d.

is

- ldconfig wird nur aufgerufen, wenn ein /lib-Verzeichnis neuer als /etc/ld.so.cache ist; ggf. wird es im Hintergrund gestartet. Der Aufruf von ldconfig lässt sich erzwingen, wenn die Umgebungsvariable run_ldconfig auf true gesetzt wird; es ist möglich, bereits am Bootprompt "run_ldconfig=true" zu setzen.

- Das Paket apache ist aufgeteilt worden. Installieren Sie auch die mod_*-Unterpakete, wenn Sie spezielle Erweiterungen benötigen. Die Dokumentation zu PHP finden Sie im Paket phpdoc. Die Logdateien sind aus Gründen der Übersichtlichkeit in /var/log/httpd zu finden.

- Paket openssh: Um die Sicherheit zu erhöhen, ist „X11-forwarding" standardmäßig ausgeschaltet. Mit dem Parameter -X kann dies Feature eingeschaltet werden. In /etc/ssh/ssh_config kann durch den Eintrag von ForwardX11 yes das Forwarding global oder nur für bestimmte Rechner eingeschaltet werden. Benutzer können diese Option auch in ~/.ssh/config setzen.

- ypserv aus dem Paket ypserv ist nicht länger gegen die „tcp-wrapper"-Bibliothek gelinkt, sondern benutzt /var/yp/securenets. Nach einem Update sollten die Einstellungen aus /etc/hosts.allow bzw. aus /etc/hosts.deny nach /var/yp/securenets übernommen werden.

- Der Portmapper wird (seit SuSE Linux 7.1) über /etc/init.d/portmap) bzw. mit rcportmap gestartet; /sbin/init.d/rpc ist nunmehr obsolete.

- Zum Paket cron: Wie es der FHS verlangt, liegen die cron-Tabellen unter /var/spool/cron/tabs; vgl. Abschnitt *Paket cron* auf Seite 198.

- Zum Paket postgres: PostgreSQL und all die zugehörigen Komponenten sind konsequent in Anlehnung an die Originalpakete aufgeteilt worden. Paket pg_datab mit der Initialisierungsdatenbank ist nicht mehr notwendig; die Initialisierung erledigt im Bedarfsfall das Startskript.

- Zum Paket mutt: Zahlreiche Einzelheiten haben sich geändert. Die Konfigurationsdateien /etc/Muttrc und /etc/skel/.muttrc versu-

chen soweit möglich das gewohnte Verhalten zu bewahren; in .muttrc sorgen die Zeilen

```
set autoedit=yes
set edit_headers=yes
```

dafür, dass sofort der Editor gestart wird, wenn eine Mail geschrieben werden soll. Andererseits gibt es gewichtige Änderungen, die ein neues Verhalten erfordern (z. B. bei PGP). Bitte lesen Sie die mitgelieferte Dokumentation.

Von 7.0 auf 7.1

Probleme und Besonderheiten:
http://sdb.suse.de/sdb/de/html/bugs71.html.

- *Kernel:* Die „low-level"-Treiber für spezielle EIDE-Chipsätze sind in den Standardkernel integriert; k_eide bzw. eide sind als separate Images nicht mehr notwendig. Mithin entfällt das Erstellen einer eigenen Bootdiskette, wenn man auf diese Treiber angewiesen ist.
- Die Bedeutung der *Runlevel* hat sich geändert; vgl. Tabelle 11.1 auf Seite 228. Die init-Skripten liegen nun in /etc/init.d; falls eigene Skripten erstellt wurden, sollten diese vor dem Update gesichert werden.
- DEFAULT_LANGUAGE: Neuer Name für die ehemalige Variable LANGUAGE in der /etc/rc.config (seit SuSE Linux 8.0 in /etc/sysconfig/language); vgl. Abschnitt *Lokale Anpassungen – I18N/L10N* auf Seite 220.
- Die /etc/resolv.conf wird direkt von YaST bzw. YaST2 geschrieben; nicht mehr von SuSEconfig. Seit Version 7.2 übernimmt diese Aufgabe das Skript /sbin/modify_resolvconf aus dem Paket aaa_base.
- Die Beschränkung der Paketnamen auf 8 Zeichen ist gefallen und viele Pakete konnten eingängige Namen bekommen.
- Die Funktionalität des Pakets dochost wurde in das Paket susehelp übernommen; dochost ist damit obsolete.
- Zum ehemaligen Paket ypclient: Dies Paket ist nunmehr in die Pakete ypbind und yp-tools aufgeteilt und das Init-Skript heißt ypbind.
- Zum Paket jade_dsl: Um einen Konflikt mit dem Paket rzsz zu vermeiden, heißt das Kommandozeilentool sx nun s2x bzw. sgml2xml.

Von 7.1 auf 7.2

Probleme und Besonderheiten:
http://sdb.suse.de/sdb/de/html/bugs72.html.

- Paket nkitb, wie zuvor bereits Paket nkita, ist aufgelöst; die einzelnen Programme sind in den Paketen talk, rsh, finger, rwho, telnet usw. und den entsprechenden -server-Paketen leicht zu finden. In Paket iputils ist beispielsweise ping enthalten.

  Einige Programme sind bereits „IPv6 ready“ . Achten Sie deshalb darauf, dass DNS richtig konfiguriert ist – andernfalls kann es passieren, dass der DNS-Timeout für IPv6-Anfrage abgewartet werden muss; in /etc/nsswitch.conf ist die Option dns durch dns6 zu ersetzen.

- Umbenennung weiterer Pakete (vgl. dazu auf der vorherigen Seite); z. B.:
  Paket docbook-dsssl-stylesheets, Paket docbook_3 und Paket docbook_4.

- Das Paket mod_php4 ist nun anstelle von mod_php zu installieren.

- Die Bestandteile des Emacs' sind auf mehrere Pakete verteilt:

  - Basispaket emacs.
  - Dazu ist in der Regel das Paket emacs-x11 zu installieren, in dem das Programm *mit* X11-Unterstützung enthalten ist.
  - Im Paket emacs-nox ist das Programm *ohne* X11-Unterstützung enthalten.
  - Paket emacs-info: Online-Dokumentation im Info-Format.
  - Paket emacs-el enthält die nicht kompilierten Bibliotheksdateien in Emacs Lisp – zur Laufzeit nicht erforderlich!
  - Zahlreiche Zusatzpakete, die nach Bedarf installiert werden können: Paket emacs-auctex (für LaTeX); Paket psgml (für SGML/XML); Paket gnuserv (für Client-/Serverbetrieb) usw.

- Änderungen im Zusammenhang mit dem FHS (vgl. Abschnitt *Filesystem Hierarchy Standard (FHS)* auf Seite 196):

  - /media (war /cdrom und /floppy)

  Für eine Übergangszeit stehen Kompatibilitätslinks zur Verfügung.

Von 7.2 auf 7.3

Probleme und Besonderheiten:
`http://sdb.suse.de/sdb/de/html/bugs73.html`.

- Beim Kernel 2.4, der mit SuSE Linux ausgeliefert wird, ist nunmehr IDE-DMA eingeschaltet. Sollte es im Zusammenhang mit DMA zu Schwierigkeiten kommen, können Sie auf die Startoption 'Installation - Safe Settings' ausweichen; vgl. auf Seite 9.
- Unabhängig von der `rc.config`-Variablen `DISPLAYMANAGER` (seit SuSE Linux 8.0 in `/etc/sysconfig/displaymanager`) ist dafür zu sorgen, dass der gewünschte Runlevel in `/etc/inittab` eingetragen ist. YaST2 kann dies sicherstellen; vgl. Abschnitt *Runlevel-Editor* auf Seite 84.
- Samba: Die Konfigurationsdateien sind in das Verzeichnis `/etc/samba` verschoben worden, um die Übersichtlichkeit zu erhöhen.
- MySQL verwendet nun die TCP-Wrapper-Bibliothek, um die Sicherheit zu erweitern.

  Das neue Unterpaket `mysql-Max` beinhaltet die neuen bzw. erweiterten Features; diese stehen nach Installation des Paketes automatisch zur Verfügung.
- Um Platz zu sparen (mehr als 30 MB), wird das Paket `allman` nicht mehr mitgeliefert; die Manual-Pages sind jedoch weiterhin bei den jeweiligen Paketen dabei.
- DocBook-Dokumente, die bestimmte „Features" verwenden, werden von `db2x.sh` akzeptiert (Paket `docbktls`). Wer auf kompatible Dokumente angewiesen ist, sollte mit der Option `--strict` arbeiten.

Von 7.3 auf 8.0

Probleme und Besonderheiten:
`http://sdb.suse.de/sdb/de/html/bugs80.html`.

- Bootdisketten werden nur noch in Form von Diskettenimages (Verzeichnis `disks`) mitgeliefert. Eine Bootdiskette benötigen Sie nur, wenn Sie nicht von CD booten können; je nach Hardware oder Installationsvorhaben sind zusätzlich Disketten von den Images `modules1` (früher `modules`) bzw. `modules2` zu erstellen; zum Vorgehen vgl. *Bootdiskette*

unter DOS erstellen auf Seite 21 bzw. *Bootdiskette unter einem unix-artigen System erstellen* auf Seite 22.

- YaST2 ersetzt nunmehr vollständig YaST1, auch im Text- bzw. Konsolenmodus.
- Einige BIOSse benötigen den Kernelparameter `realmode-power-off`; dieser hieß bis Kernelversion 2.4.12 `real-mode-poweroff`.
- Die `START`-Variablen der `rc.config` zum Starten von Diensten sind nicht mehr erforderlich. Alle Dienste werden gestartet, wenn die entsprechenden Links in den Runlevel-Verzeichnissen vorhanden sind; die Links werden mit `insserv` angelegt.
- Systemdienste werden über Variablen-Einträge in den Dateien in `/etc/sysconfig` konfiguriert; beim Update werden die Einstellungen aus den Dateien in `/etc/rc.config.d` übernommen.
- `/etc/init.d/boot` in mehrere Skripte aufgeteilt und, wenn sinnvoll, in andere Pakete verschoben (vgl. Paket `kbd`, Paket `isapnp`, Paket `lvm` usw.); vgl. auf Seite 231.
- Im Bereich Netzwerk wurde eine Reihe von Änderungen vorgenommen; vgl. dazu Abschnitt *Die Einbindung ins Netzwerk* auf Seite 284.
- Zur Verwaltung der Protokoll-Dateien (engl. *logfiles*) wird das logrotate verwendet; `/etc/logfiles` ist nicht mehr erforderlich; vgl. Abschnitt *Protokoll-Dateien – das Paket logrotate* auf Seite 198.
- Das Login für `root` per telnet oder rlogin kann durch Einstellungen in den Dateien in `/etc/pam.d` erlaubt werden; das Setzen von `ROOT_LOGIN_REMOTE` auf `yes` wird wegen Sicherheitsaspekten nicht mehr zugelassen.
- `PASSWD_USE_CRACKLIB` kann mit YaST2 aktiviert werden.
- Wenn NIS-Dateien für `autofs` über NIS verteilt werden sollen, ist das NIS-Client-Modul von YaST2 zur Konfiguration zu verwenden; aktivieren Sie dort 'Automounter starten'. Dadurch ist die Variable `USE_NIS_FOR_AUTOFS` obsolet.
- locate zum schnellen Finden von Dateien gehört nicht mehr zum Standardumfang der installierten Software. Bei Bedarf bitte nachinstallieren – dann wird auch wie früher automatisch ca. 15 Minuten nach dem Einschalten der updatedb-Prozess gestartet!

- Für pine ist Maus-Support aktiviert. Das bedeutet, dass man Pine in einem xterm (o. Ä.) auch mit der Maus bedienen kann, wenn man auf die Menüpunkte klickt. Das bedeutet allerdings auch weiterhin, dass Cut & Paste nur bei gedrückter Shift-Taste funktioniert, wenn der Mouse-Support aktiv ist. Bei einer Neuinstallation ist dies deaktiviert. Beim Update ist jedoch nicht auszuschließen, dass diese Funktion aktiv ist (wenn eine älter `~/.pinerc` vorhanden ist). In diesem Fall kann man in der Pine-Konfiguration die Option `enable-mouse-in-xterm` deaktivieren und alles ist wieder gut.

Von 8.0 auf 8.1

Probleme und Besonderheiten:
`http://sdb.suse.de/sdb/de/html/bugs81.html`.

- Änderungen bei Benutzer- und Gruppennamen des Systems: Um Übereinstimmung mit UnitedLinux zu erreichen, wurden einige Einträge in `/etc/passwd` bzw. `/etc/group` angepasst.
    - ▷ Geänderte Benutzer: `ftp` nun in Gruppe `ftp` (nicht mehr in `daemon`).
    - ▷ Umbenannte Gruppen: `www` (war `wwwadmin`); `games` (war `game`).
    - ▷ Neue Gruppen: `ftp` (mit GID `50`); `floppy` (mit GID `19`); `cdrom` (mit GID `20`); `console` (mit GID `21`); `utmp` (mit GID `22`).
- Änderungen im Zusammenhang mit dem FHS (vgl. Abschnitt *Filesystem Hierarchy Standard (FHS)* auf Seite 196):
    - ▷ Eine Beispiel-Umgebung für HTTPD (Apache) wird unter `/srv/httpd` angelegt (war `/usr/local/httpd`).
    - ▷ Eine Beispiel-Umgebung für FTP wird unter `/srv/ftp` angelegt (war `/usr/local/ftp`)
- Um einen gezielten Zugriff auf gesuchte Software zu ermöglichen, sind die einzelnen Pakete nicht mehr in wenigen unübersichtlichen Serien untergebracht, sondern in eingängigen „RPM-Gruppen“. Das hat zur Konsequenz, dass es auf den CDs keinen kryptischen Verzeichnisse unter `suse` mehr gibt, sondern nur noch wenige nach Architekturen benannte Verzeichnisse wie z. B. `ppc`, `i586` oder `noarch`.
- Bei einer Neuinstallation werden nunmehr die folgenden Programme eingerichtet bzw. nicht mehr automatisch installiert:

- ▷ Der Bootloader GRUB, der entschieden mehr Möglichkeiten als LILO bietet. LILO bleibt jedoch erhalten, wenn ein *Update* des Systems durchgeführt wird.
- ▷ Der Mailer postfix anstelle von sendmail.
- ▷ Anstelle von majordomo wird die moderne Mailinglistensoftware mailman installiert.
- ▷ harden_suse bitte von Hand bei Bedarf auswählen und die aktuelle Dokumentation dazu lesen!

- Aufgeteilte Pakete: `rpm` in `rpm` und `rpm-devel`; `popt` in `popt` und `popt-devel`; `libz` in `zlib` und `zlib-devel`.

  `yast2-trans-*` nun nach Sprachen aufgeteilt: `yast2-trans-cs` (tschechisch), `yast2-trans-de` (deutsch), `yast2-trans-es` (spanisch) etc.; bei der Installation werden nicht mehr alle Sprachen installiert, um Plattenplatz zu sparen. Bei Bedarf die notwendigen Pakete für die YaST2-Sprachunterstützung bitte nachinstallieren!

- Umbenannte Pakete: `bzip` in `bzip2`.
- Nicht mehr mitgelieferte Pakete: `openldap`, bitte nun `openldap2` verwenden.

RPM – Der Paket-Manager der Distribution

Bei SuSE Linux kommt RPM (`rpm`) (engl. *RPM Package Manager*) als Paket-Management zum Einsatz. Damit steht den Benutzern, den Systemadministratoren und nicht zuletzt den Pakete-Macher die mächtige RPM-Datenbank zur Verfügung, über die jederzeit detaillierte Informationen zur installierten Software abgefragt werden können.

Im Wesentlichen kann `rpm` in drei Modi agieren: installierbare Pakete aus den unangetasteten Quellen (engl. *pristine sources*) herstellen, diese Pakete installieren bzw. auch wieder sauber de-installieren oder updaten sowie Anfragen an die RPM-Datenbank bzw. an einzelne RPM-Archive richten.

Installierbare RPM-Archive sind in einem speziellen binären Format gepackt; die Archive bestehen aus den zu installierenden (Programm-)Dateien und aus verschiedenen Meta-Informationen, die während der Installation von `rpm` benutzt werden, um das jeweilige Softwarepaket zu konfigurieren, oder die zu Dokumentationszwecken in der RPM-Datenbank abgelegt werden. RPM-Archive haben die Dateinamen-Endung `.rpm`.

Mit rpm lassen sich LSB-konforme Pakete verwalten; zu LSB vgl. Abschnitt *Linux Standard Base (LSB)* auf Seite 196.

Tipp

Bei etlichen Paketen sind die für die Software-Entwicklung notwendigen Komponenten (Bibliotheken, Header- und Include-Dateien etc.) in eigene Pakete ausgelagert. Diese Entwicklungspakete werden nur benötigt, wenn Sie Software *selbst* übersetzen (compilieren) wollen – beispielsweise neuere GNOME-Pakete. Diese Entwicklungspakete sind in der Regel an dem Namenszusatz `-devel` (früher: `dev` oder `d`) zu erkennen: Paket `alsa-devel`, Paket `gimp-devel`, Paket `kdelibs-devel` etc.

Tipp

Prüfen der Authentizität eines Pakets

Seit der Version 7.1 sind RPM-Pakete von SuSE mit GnuPG signiert:

```
1024D/9C800ACA 2000-10-19 SuSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F  9994 A84E DAE8 9C80 0ACA
```

Mit dem Befehl

```
erde:~ #  rpm --verbose --checksig apache-1.3.12.rpm
```

kann man die Signatur eines RPM-Pakets überprüfen und so feststellen, ob es wirklich von SuSE oder einer anderen vertrauenswürdigen Stelle stammt; insbesondere bei Updatepaketen, die man aus dem Internet lädt, ist dies zu empfehlen. Unser öffentlicher Paketsignierschlüssel ist standardmäßig in `/root/.gnupg/` hinterlegt.

Pakete verwalten: Installieren, Updaten und Deinstallieren

Im Normalfall ist das Installieren eines RPM-Archivs schnell erledigt:

```
erde:~ #  rpm -i ⟨paket⟩.rpm
```

Mit diesem Standardbefehl wird ein Paket aber nur dann installiert, wenn die „Abhängigkeiten“ erfüllt sind und wenn es zu keinen „Konflikten“ kommen kann; rpm fordert per Fehlermeldung die Pakete an, die zum Erfüllen der Abhängigkeiten notwendig sind. Die Datenbank wacht im Hintergrund darüber, dass es zu keinen Konflikten kommt: eine Datei darf in der Regel nur

zu einem Paket gehören. Mit verschiedenen Optionen kann man sich über diese Regel hinwegsetzen – wer dies tut, der sollte aber genau wissen, was er tut, da er damit eventuell die Updatefähigkeit des Systems aufs Spiel setzt.

Interessant ist auch die Option `-U` bzw. `--upgrade`, um ein Paket zu aktualisieren. Dadurch wird eine ältere Version des gleichen Pakets gelöscht und dann die neue Version installiert. Gleichzeitig versucht `rpm`, sorgfältig mit den *Konfigurationsdateien* umzugehen, wobei – etwas vereinfacht – die folgende Strategie zum Tragen kommt:

- Falls eine Konfigurationsdatei vom Systemadministrator *nicht* verändert wurde, dann wird von `rpm` die neue Version der entsprechenden Datei installiert. Es sind keine Eingriffe seitens des Administrators notwendig.
- Falls eine Konfigurationsdatei vom Administrator zu einem Zeitpunkt vor dem Update geändert wurde, dann wird `rpm` die geänderte Datei dann – und nur dann – mit der Erweiterung `.rpmorig` oder `.rpmsave` sichern und die neue Version aus dem RPM-Paket installieren, wenn sich zwischen ursprünglicher Datei und der Datei aus dem Update-Paket etwas geändert hat. In diesem Fall ist es sehr wahrscheinlich, dass Sie die frisch installierte Konfigurationsdatei anhand der Kopie (`.rpmorig` oder `.rpmsave`) auf Ihre System-Bedingungen hin abstimmen müssen.
- `.rpmnew`-Dateien werden immer dann auftauchen, wenn es die Konfigurationsdatei bereits gibt *und* wenn in der `.spec`-Datei die `noreplace`-Kennung gesetzt wurde.

Im Anschluss an ein Update sollten nach dem Abgleich alle `.rpmorig`-, `.rpmsave`- bzw. `.rpmnew`-Dateien unbedingt entfernt werden, um kommenden Updates nicht als Hindernis im Wege zu liegen. Die Erweiterung `.rpmorig` wird gewählt, wenn die Datei der RPM-Datenbank noch nicht bekannt war, sonst kommt `.rpmsave` zum Zuge; mit anderen Worten: `.rpmorig`s entstehen beim Update von Fremdformat auf RPM und `.rpmsave` beim Update von RPM-alt auf RPM-neu. Bei `.rpmnew` kann keine Aussage gemacht werden, ob vom Systemadministrator eine Änderung an der Konfigurationsdatei vorgenommen wurde oder ob nicht.

Beachten Sie, dass einige Konfigurationsdateien (z. B. `/etc/httpd/httpd.conf`) mit Absicht nicht überschrieben werden, um den sofortigen Weiterbetrieb mit den eigenen Einstellungen zu ermöglichen.

Die Option `-U` ist also mehr als ein Äquivalent für die Abfolge `-e` (Deinstallieren/Löschen) und `-i` (Installieren). Wann immer möglich, dann ist der Option `-U` der Vorzug zu geben.

Hinweis

Nach jedem Update müssen Sie die von `rpm` angelegten Sicherungskopien mit der Erweiterung `.rpmorig` oder `.rpmsave` kontrollieren; das sind Ihre alten Konfigurationsdateien. Falls erforderlich, übernehmen Sie bitte Ihre Anpassungen aus den Sicherungskopien in die neuen Konfigurationsdateien, und löschen Sie dann die alten Dateien mit der Erweiterung `.rpmorig` bzw. `.rpmsave`.

Hinweis

Wenn ein Paket entfernt werden soll, geht man ähnlich geradlinig vor:

```
erde:~ #  rpm -e ⟨paket⟩
```

`rpm` wird ein Paket aber nur dann entfernen, wenn keine Abhängigkeiten mehr bestehen; so ist es z. B. theoretisch nicht möglich, Tcl/Tk zu löschen, solange noch irgendein anderes Programm Tcl/Tk benötigt – auch darüber wacht RPM mithilfe der Datenbank.

Falls in einem Ausnahmefall eine derartige Lösch-Operation nicht möglich sein sollte, obwohl *keine* Abhängigkeiten mehr bestehen, dann kann es hilfreich sein, die RPM-Datenbank mittels der Option `-rebuilddb` neu aufzubauen; vgl. unten die Anmerkungen zur RPM-Datenbank (Abschnitt *Anfragen stellen* auf Seite 54).

Anfragen stellen

Mit der Option `-q` (engl. *query*) leitet man Anfragen ein. Damit ist es sowohl möglich die RPM-Archive selbst zu durchleuchten (Option `-p` ⟨*paket_datei*⟩) als auch die RPM-Datenbank zu befragen. Die Art der angezeigten Information kann man mit den zusätzlichen Optionen auswählen; vgl. Tabelle 2.1 auf der nächsten Seite.

`-i`	Paket-Informationen anzeigen
`-l`	Dateiliste des Pakets anzeigen
`-f` ⟨*DATEI*⟩	Anfrage nach Paket, das die Datei ⟨*DATEI*⟩ besitzt; ⟨*DATEI*⟩ muss mit vollem Pfad angegeben werden!
`-s`	Status der Dateien anzeigen (impliziert `-l`)
`-d`	Nur Dokumentationsdateien auflisten (impliziert `-l`)
`-c`	Nur Konfigurationsdateien auflisten (impliziert `-l`)

Tabelle 2.1: *Fortsetzung auf der nächsten Seite…*

`--dump`	Alle überprüfbaren Infos zu jeder Datei anzeigen (mit `-l`, `-c` oder `-d` benutzen!)
`--provides`	Fähigkeiten des Pakets auflisten, die ein anderes Paket mit `--requires` anfordern kann
`--requires`, `-R`	Paket-Abhängigkeiten ausgeben
`--scripts`	Die diversen (De-)Installations-Skripten ausgeben

Tabelle 2.1: *Die wichtigsten Abfrageoptionen* (`-q` [`-p`] … ⟨*paket*⟩)

Der Befehl

```
erde:~ #  rpm -q -i wget
```

gibt die Information in Ausgabe 3 aus.

```
Name        : wget                    Relocations: (not relocateable)
Version     : 1.8.1                        Vendor: SuSE AG, Nuern-
berg, Germany
Release     : 142                      Build Da-
te: Fri Apr  5 16:08:13 2002
Install date: Mon Apr  8 13:54:08 2002 Build Host: knox.suse.de
Group       : Productivity/Networking/Web/Utilities   Source RPM:
 wget-1.8.1-142.src.rpm
Size        : 2166418                     License: GPL
Packager    : feedback@suse.de
Summary     : A tool for mirroring FTP and HTTP servers
Description :
Wget enables you to retrieve WWW documents or FTP files from a server.
This might be done in script files or via command line.
[...]
```

Ausgabe 3: *rpm -q -i wget*

Die Option `-f` führt nur dann zum Ziel, wenn man den kompletten Dateinamen, einschließlich des Pfades, kennt; es dürfen beliebig viele zu suchende Dateinamen angegeben werden, z. B.:

```
erde:~ #  rpm -q -f /bin/rpm /usr/bin/wget
```

führt zu dem Ergebnis:

```
rpm-3.0.3-3
wget-1.5.3-55
```

Kennt man nur einen Teil des Dateinamens, so muss man sich mit einem Shell-Skript behelfen (vgl. Datei 1); der gesuchte Dateiname ist als Parameter beim Aufruf des Skripts zu übergeben.

```
#! /bin/sh
for i in $(rpm -q -a -l | grep  $1); do
    echo "\"$i\" ist in Paket:"
    rpm -q -f $i
    echo ""
done
```

Datei 1: *Paket-Suchskript*

Mit dem Befehl

```
erde:~ #  rpm -q -changelog rpm
```

kann man sich gezielt die Auflistung der Informationen (Updates, Konfiguration, Änderungen etc.) zu einem bestimmten Paket anzeigen lassen; hier beispielsweise zu dem Paket *rpm*. Es werden allerdings nur die letzten 5 Einträge in der RPM-Datenbank installiert, um Platz für das installierte System zu sparen; im Paket selbst sind alle Einträge (der letzten 2 Jahre) enthalten – diese Abfrage funktioniert, wenn CD 1 unter `/cdrom` eingehangen ist:

```
erde:~ #  rpm -qp -changelog /cdrom/suse/a1/rpm.rpm
```

Anhand der installierten Datenbank lassen sich auch Überprüfungen durchführen; eingeleitet werden diese Vorgänge mit der Option `-V` (gleichbedeutend mit `-y` oder `--verify`). Damit veranlasst man `rpm`, all die Dateien anzuzeigen, die sich im Vergleich zur ursprünglichen Version, wie sie im Paket enthalten war, geändert haben. `rpm` stellt dem eigentlichen Dateinamen bis zu acht Zeichen voran, die auf folgende Änderungen hinweisen:

`5`	MD5-Prüfsumme
`S`	Dateigröße
`L`	Symbolischer Link
`T`	Modification Time
`D`	„major“ und „minor“ Gerätenummer (engl. *device number*)
`U`	Benutzer (engl. *user*)
`G`	Gruppe (engl. *group*)
`M`	Modus (einschl. Rechte und Typus)

Tabelle 2.2: *Die Überprüfungen*

Bei Konfigurationsdateien wird zusätzlich ein `c` ausgegeben. Beispiel, falls etwas an `/etc/wgetrc` aus dem Paket `wget` geändert wurde:

```
erde:~ #  rpm -V wget

S.5....T c /etc/wgetrc
```

Die Dateien der RPM-Datenbank liegen unter `/var/lib/rpm`. Bei einer `/usr`-Partition von 1 GB kann die Datenbank durchaus 30 MB Plattenplatz beanspruchen; insbesondere nach einem kompletten Update. Falls die Datenbank über Gebühr groß erscheint, ist es meist hilfreich, mit der Option `--rebuilddb` eine neue Datenbank auf Basis der existierenden zu erstellen; es ist sinnvoll, vor einem solchen „Rebuild" eine Kopie der existierenden Datenbank aufzubewahren.

Weiterhin legt das `cron`-Skript `cron.daily` täglich gepackte Kopien der Datenbank unter `/var/adm/backup/rpmdb` an, deren Anzahl durch die Variable ⟨*MAX_RPMDB_BACKUPS*⟩ (Standard: `5`) in der `/etc/rc.config` vorgegeben wird; es ist mit bis zu 3 MB pro Backup zu rechnen (bei einer 1 GB großen `/usr`). Dieser Platzverbrauch ist bei Bestimmung der Größe der Root-Partition unbedingt zu berücksichtigen, falls man für `/var` keine eigene Partition vorsehen will.

Quellpakete installieren und kompilieren

Alle Quellpakete (engl. *Sources*) der SuSE Linux haben die Erweiterung `.spm` hinter dem eigentlichen Paketnamen; diese Dateien sind die sog. „Source-RPMs".

Tipp

Diese Pakete können mit YaST – wie jedes andere Paket – installiert werden; allerdings werden Quellpakete nie als installiert (`[i]`) markiert wie die „regulären" anderen Pakete. Dies liegt daran, dass die Quellpakete nicht in die RPM-Datenbank aufgenommen werden; in der RPM-Datenbank nämlich erscheint nur *installierte* Betriebssoftware.

Tipp

Die Arbeitsverzeichnisse des rpm unter `/usr/src/packages` müssen vorhanden sein (falls keine eigenen Einstellungen wie etwa via `/etc/rpmrc` vorgenommen wurden):

`SOURCES` für die originalen Quellen (`.tar.gz`-Dateien etc.) und für die distributionsspezifischen Anpassungen (`.dif`-Dateien).

SPECS für die .spec-Dateien, die in der Art eines Meta-Makefiles den „build"-Prozess steuern.

BUILD unterhalb dieses Verzeichnisses werden die Quellen entpackt, gepatcht und kompiliert.

RPMS hier werden die fertigen „Binary"-Pakete abgelegt.

SRPMS und hier die „Source"-RPMs.

Hinweis

Bitte machen Sie keine RPM-Experimente mit wichtigen System-Komponenten (Paket glibc, Paket rpm, Paket sysvinit etc.); Sie setzen die Funktionstüchtigkeit Ihres Systems aufs Spiel.

Hinweis

Wenn Sie ein Quellpaket mit YaST installieren, dann werden die für den „build"-Prozess notwendigen Komponenten unter /usr/src/packages installiert: die Quellen und die Anpassungen unter SOURCES und die dazugehörige .spec-Datei unter SPECS. Zum „Pakete-Machen" (engl. *build mode*) vgl. [Bai97]; dort, oder auch in der Manual-Page von rpm (man rpm), werden weitere Einsatzmöglichkeiten vorgestellt.

Im Folgenden wird das Paket wget.spm betrachtet. Nachdem das Quellpaket wget.spm mit YaST installiert wurde, gibt es die Dateien:

```
/usr/src/packages/SPECS/wget.spec
/usr/src/packages/SOURCES/wget-1.4.5.dif
/usr/src/packages/SOURCES/wget-1.4.5.tar.gz
```

Mit rpm -b ⟨*X*⟩ /usr/src/packages/SPECS/wget.spec wird der Kompiliervorgang angestoßen; dabei kann ⟨*X*⟩ für verschiedene Stufen stehen (vgl. die --help-Ausgabe bzw. die RPM-Dokumentation); hier nur eine kurze Erläuterung:

-bp Quellen im Verzeichnis /usr/src/packages/BUILD präparieren: entpacken und patchen

-bc wie -bp, jedoch zusätzlich noch kompilieren

-bi wie -bc, jedoch zusätzlich noch installieren; Achtung, wenn ein Paket nicht das BuildRoot-Feature unterstützt, ist es möglich, dass Sie sich während dieses Installationsvorgangs wichtige Konfigurationsdateien überschreiben!

-bb wie -bi, jedoch zusätzlich noch das sog. Binary-RPM herstellen; bei Erfolg liegt es in /usr/src/packages/RPMS.

-ba wie -bb, jedoch zusätzlich noch das sog. Source-RPM herstellen; bei Erfolg liegt es in /usr/src/packages/SRPMS.

Mit der Option -short-circuit lassen sich einzelne Schritte überspringen.

Das hergestellte Binary-RPM ist schließlich mit rpm -i oder besser mit rpm -U zu installieren, damit es auch in der RPM-Datenbank auftaucht.

Tools für RPM-Archive und die RPM-Datenbank

Der Midnight Commander (mc) ist in der Lage, den Inhalt eines RPM-Archivs anzuzeigen bzw. Teile daraus zu kopieren. Er bildet ein solches Archiv als ein virtuelles Dateisystem ab, sodass alle gewohnten Menüpunkte des Midnight Commander – wenn sinnvoll – zur Verfügung stehen: Die Kopfzeilen-Informationen der „Datei“ HEADER kann man sich mit F3 ansehen; mit den Cursor-Tasten und Enter lässt sich durch die Struktur des Archivs „browsen“, um bei Bedarf mit F5 Komponenten herauszukopieren. – Übrigens, mittlerweile gibt es auch für den Emacs ein rpm.el, ein „Frontend“ für rpm

xrpm heißt ein grafischer RPM-Manager; realisiert ist dieses Tool in Python, einer eleganten Skript-Sprache. xrpm unterstützt Aktionen per FTP.

KDE enthält das Tool krpm, ein grafisches Interface unter X, um RPM zu bedienen. Bei GNOME finden Sie gnorpm.

Mit Alien (alien) ist es möglich, die Paketformate der verschiedenen Distributionen zu konvertieren. So kann man versuchen, alte TGZ-Archive *vor* dem Installieren nach RPM umzuwandeln, damit *während* der Installation die RPM-Datenbank mit den Paket-Informationen versorgt wird. Aber Achtung: alien ist ein Perl-Skript und befindet sich nach Angaben der Programm-Autoren noch in einem Alpha-Stadium – wenngleich es bereits eine hohe Versionsnummer erreicht hat.

Last, not least – es gibt YaST2 (vgl. auch Abschnitt *Software* auf Seite 66).

Teil II

Konfiguration

YaST2 im Textmodus (ncurses)

Dieses Kapitel richtet sich v. a. an Systemadministratoren und Experten, auf deren Rechner kein X-Server läuft und die auf das textbasierte Installationswerkzeug angewiesen sind.

Sie erhalten in diesem Kapitel grundlegende Informationen zum Aufruf und zur Bedienung von YaST2 im Textmodus (ncurses). Zudem erfahren Sie, wie Sie Ihr System automatisch online aktualisieren können und so immer auf dem neuesten Stand halten.

Erläuterungen zu ncurses 60
Aufruf und Bedienung 60
Bedienung der Module 62
Aufruf der einzelnen Module 63
Das YaST Online Update 63

Erläuterungen zu ncurses

Nachdem die Weiterentwicklung von YaST1 eingestellt werden musste, tritt an dessen Stelle die textbasierte Version von YaST2. Obwohl diese bereits mit ausgeliefert wurde, wurde sie jedoch kaum verwendet. Ein Grund ist sicher, dass viele sich an die Bedienung von YaST1 gewöhnt haben und irritiert sind, da YaST2-ncurses ein anderes Look-and-Feel mit sich bringt sowie gewohnte Shortkeys aus YaST1 nicht mehr funktionieren. Die Bedienung von YaST2 im Textmodus erfolgt wie bei YaST1 ebenfalls per Tastatur.

Aufruf und Bedienung

Um YaST2 im Textmodus zu starten, müssen Sie als `root` am Prompt eingeben:

```
erde: # yast
```

Die Bedienung ist zwar ungewohnt, aber sehr einfach. Mit den Tasten Tab, Alt + Tab, Leertaste, Pfeiltasten (↑ und ↓) und Enter sowie mit Shortcuts lässt sich im Prinzip das ganze Programm bedienen. Wenn Sie YaST2 im Textmodus starten, erscheint zuerst das Hauptfenster (siehe Abb. 3.1).

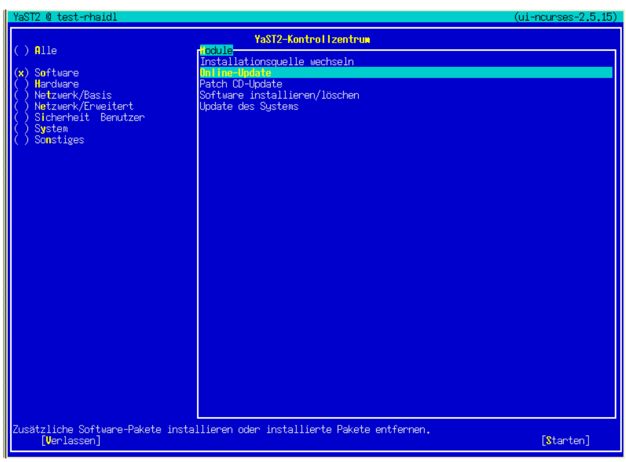


Abbildung 3.1: *Das Hauptfenster von YaST2-ncurses mit aktivem Modulrahmen*

Sie sehen hier drei Bereiche: In der linken Spalte sehen Sie die Kategorien, in denen die verschiedenen Module eingeordnet sind. Rechts sind die jeweiligen

Module der Kategorie (jener, die mit einem (**x**) ausgewählt ist) in einem weißen Rahmen. Unten sind die beiden Buttons zum Verlassen bzw. zum Starten des im rechten Rahmen markierten Moduls.

Nach dem Start steht der Cursor auf dem obersten Feld 'Alle' bzw. ist dieses Feld farbig (i. d. R. grün) unterlegt. Ausgewählt ist jedoch 'Software', erkenntlich an dem "**x**" in der Klammer. Mit Tab wechseln Sie nun in der linken Spalte von einem Punkt zum nächsten. Sie aktivieren die Kategorie, die grün unterlegt ist, mit der Leertaste. Sie sehen dann, dass im rechten Rahmen die jeweiligen Module dieser Kategorie erscheinen. Die Farbe der markierten Punkte ist abhängig von den Einstellungen des Terminals, das sie benutzen.

Drücken Sie nun so oft Tab, bis der dünne weiße Rahmen rechts verstärkt hervortritt. Alternativ können Sie im Regelfall (siehe Abschnitt *Bedienung der Module* auf der nächsten Seite) auch mit der Tastenkombination Alt + Tab oder mit ⇑ + Tab zurückspringen. Jetzt haben Sie den Kategorie-Bereich verlassen und befinden sich in dem rechten Fenster, um ein Modul zum Starten auszuwählen. Hier bewegen Sie sich nun mit den Pfeiltasten zwischen den Modulen hin und her. Ist Ihr gewünschtes Modul grün unterlegt, starten Sie dieses mit Enter. Alternativ können Sie Sie mit Tab den Modulrahmen verlassen und landen unten auf dem Button 'Verlassen'. Hier können Sie YaST beenden. Ein weiterer Druck auf Tab bringt Sie zum Button 'Starten'. Hier starten Sie nun mit Enter das ausgewählte Modul. Verschiedene Buttons oder Auswahlfelder enthalten auch einen andersfarbigen (bei Standardeinstellungen gelben) Buchstaben. Mit der Kombination Alt + gelberBuchstabe können Sie den jeweiligen Button ohne umständliche TAB-Navigation direkt anwählen.

Einschränkung der Tastenkombinationen

Sollten auf Ihrem System bei laufendem X-Server systemweite Alt-Tastenkombinationen bestehen, kann es sein, dass die Alt-Kombinationen im YaST nicht funktionieren. Außerdem können Tasten wie Alt oder ⇑ durch Einstellungen des benutzten Terminals vorbelegt sein.

Ersatz von Alt durch Esc: Alt-Shortcuts können mit Esc anstatt Alt durchgeführt werden, z. B. ersetzt Esc + h Alt + h.

Ersatz von Vor- und Zurückspringen mittels Ctrl + f und Ctrl + b: Falls Alt- und ⇑-Kombinationen durch den Windowmanager oder das Terminal vorbelegt sind, können Sie hier alternativ die Kombinationen Ctrl + f (vorwärts) und Ctrl + b (zurück) verwenden.

Einschränkung von Funktionstasten: In SuSE Linux 8.1 sind auch die F-Tasten mit Funktionen belegt (siehe Abschnitt *Bedienung der Module* auf dieser Seite). Auch hier können bestimmte F-Tasten durch die Wahl des Terminals vorbelegt sein und daher nicht für YaST zur Verfügung stehen. Auf einer reinen Textkonsole sollten allerdings die Alt-Tastenkombinationen und die F-Tasten stets in vollem Umfang verfügbar sein.

Im folgenden wird bei der Beschreibung zur besseren Übersicht davon ausgegangen, dass die Alt-Tastenkombinationen funktionieren.

Bedienung der Module

Navigation zwischen Buttons und Auswahllisten: Mit Tab und Alt + Tab navigieren Sie jeweils zwischen den Buttons und den Rahmen von Auswahllisten hin und her.

Navigation in Auswahllisten: In einem aktivierten Rahmen, in dem sich eine Auswahlliste befindet, springen Sie immer mit den Pfeiltasten (↑ und ↓) zwischen den einzelnen Elementen, z. B. zwischen den einzelnen Modulen einer Modulgruppe im Kontrollzentrum.

Ankreuzen von Radiobuttons und Checkboxen Die Auswahl von Buttons mit einer leeren eckigen Klammer (Checkbox) oder im Kontrollzentrum links die Modulgruppen mit runden Klammern (Radiobuttons) erfolgt ebenso wie das Anwählen von Paketen bei der Paketinstallation mit Leertaste oder Enter. Das Anwählen der Buttons am unteren Rand der einzelnen Module oder des Kontrollzentrums erfolgt mit Enter, wenn Sie ausgewählt (grün unterlegt) sind, bzw. schneller mit der Kombination Alt + gelbeTaste (vgl. Abb. 3.2 auf der nächsten Seite).

Die Funktionstasten: Die F-Tasten (F1 bis F12) sind ebenfalls mit Funktionen belegt. Sie dienen zur schnellen Ansprache der verschiedenen Buttons, die zur Verfügung stehen. Welche F-Tasten mit Funktionen belegt sind, hängt davon ab, in welchem Modul Sie sich in YaST befinden, da in verschiedenen Modulen verschiedene Buttons angeboten sind (z. B. Details, Infos, Add, Delete…). Für Freunde des alten YaST1 liegen z. B. die Buttons 'OK', 'Weiter' und 'Beenden' auf der Taste F10. In der Hilfe zu YaST, die Sie mit F1 erhalten, erfahren Sie die einzelnen Funktionen hinter den F-Tasten.

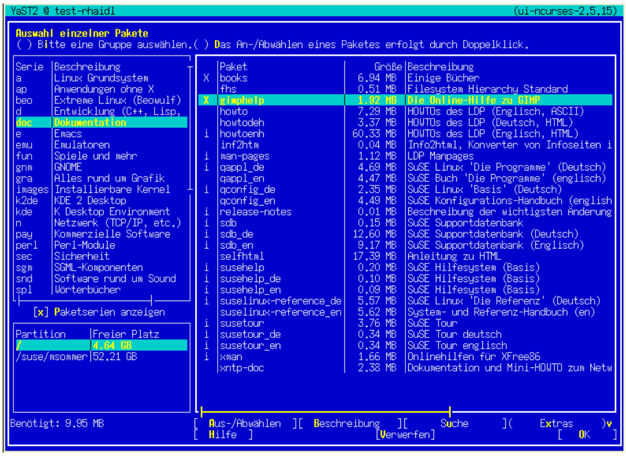


Abbildung 3.2: *Das Modul zur Softwareinstallation*

Aufruf der einzelnen Module

Zur Zeitersparnis lässt sich jedes der YaST-Module auch einzeln aufrufen. Gestartet werden die Module einfach mit dem Aufruf:

`yast` ⟨*modulname*⟩

Das Netzwerkmodul wird z. B. über `yast lan` gestartet.
Eine Liste aller Modulnamen, die auf Ihrem System zur Verfügung stehen, erhalten Sie entweder mit dem Aufruf `yast -l` oder über `yast --list`.

Die einzelnen Modulbeschreibungen finden Sie auf auf Seite 69 ff.

Das YaST Online Update

Auch das YaST Online Update (YOU) lässt sich von der Konsole aus steuern und aufrufen. Die Anleitung dazu finden Sie im Kapitel *Online-Update von der Konsole* auf Seite 67. Als Administrator kann man damit leicht einen wöchentlichen Cronjob aufsetzen, womit das System per YOU dann immer auf dem neuesten Stand bleibt.

Der Cronjob für YOU

Da nicht jeder, der YOU benutzen will/muss, mit dem Aufsetzen eines Cronjobs vertraut ist, folgt hier eine kurze Anleitung. Prinzipiell existieren zwei verschiedene Möglichkeiten für einen Cronjob. Hier soll die einfachere beschrieben werden. Folgende Schritte sind nötig:

1. Werden Sie root
2. Starten Sie den Crontabeditor mit dem Befehl `crontab -e`.
3. Tippen Sie `i` für den Insertmodus des gestarteten vi
4. Geben Sie folgende Zeilen ein:

   ```
   MAILTO=" "
   13 3 * * 0 /sbin/yast2 online_update auto.get
   53 3 * * 0 /sbin/yast2 online_update auto.install
   ```

   Die ersten 5 Stellen der beiden unteren Zeilen bedeuten jeweils von links nach rechts: 13=Minuten, 3=Stunden, *=Tag des Monat ist egal, *=Monat des Jahres ist egal, 0=Sonntag. Das heißt also, der erste Eintrag startet den Cronjob jeden Sonntag um 3 Uhr 13 nachts. Der zweite dann immer 40 Minuten später, um 3 Uhr 53. Die Zeile `MAILTO=" "` verhindert, dass root die Ausgabe von YaST2-ncurses als Mail erhält und kann natürlich weggelassen werden.

   Achtung

   Geben Sie willkürlich die Uhrzeiten für die Cronjobs ein, also bitte nicht unbedingt die Zeiten aus obigem Bespiel, da sonst zu diesem Zeitpunkt der FTP-Server sofort überlastet bzw. die Höchstzahl der gleichzeitig erlaubten Zugriffe überschritten wäre.

   Achtung

5. Speichern Sie den Cronjob mit der Tastenfolge (jeweils nacheinander eingeben) Esc `:wq` oder alternativ Esc `ZZ` ab.

Der Cron-Daemon wird automatisch neu gestartet und Ihr Cronjob in die Datei `/var/spool/cron/tabs/root` eingetragen.

YaST2 im Grafikmodus

Mit Hilfe von YaST2 können Sie SuSE Linux System um zusätzliche Hardwarekomponenten (Drucker, Soundkarte usw.) erweitern, Systemdienste, Internetzugang und Netzwerk konfigurieren sowie Software nachinstallieren oder unerwünschte Pakete löschen. In [SuS02a] finden Sie eine Beschreibung mehrerer Zugangsmöglichkeiten zu YaST2.

Der Aufruf von YaST2 66
Software 66
Hardware 69
Netzwerk/Basis 70
Netzwerk/Erweitert 71
Sicherheit und Benutzer 72
System 73
Sonstiges 84

Der Aufruf von YaST2

Sie starten YaST2 im grafischen Modus am besten über das KDE-Menüsystem. Die Bedienung kann sowohl per Maus als auch Tastatur erfolgen.

Nach dem Aufruf erscheint zunächst das YaST2 Control Center. Im linken Bereich finden Sie die Einteilung in 'Software', 'Hardware', 'Netzwerk/Basis', 'Netzwerk/Erweitert', 'Sicherheit/Benutzer', 'System' und 'Sonstiges'. Wenn Sie auf eines der Icons klicken, werden im rechten Teil die entsprechenden Module als Icons aufgelistet. Die Konfiguration in den einzelnen Modulen erfolgt meist in mehreren Schritten.

YaST2 führt Sie in den Modulen mit 'Weiter' durch alle Dialoge. Im linken Bildschirmteil erhalten Sie zum jeweiligen Thema einen Hilfetext, der Ihnen mögliche Eingaben erläutert.

Sind alle erforderlichen Angaben gemacht, schließen Sie im jeweils letzten Konfigurationsdialog den Vorgang über 'Beenden' ab. Die Konfiguration wird damit gespeichert.

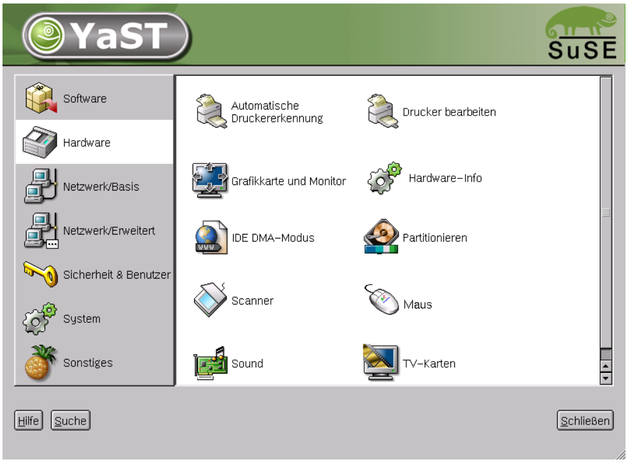


Abbildung 4.1: *YaST2 Systemkonfiguration und -administration*

Software

Wenn Sie Software nachinstallieren oder löschen wollen, haben Sie hier die Möglichkeit dazu, ebenso zum Wechsel des Installationsmediums. Ferner gibt

es zwei Update-Tools: für das „normale“ Update des Systems und für das Online-Update, das über unseren FTP-Server erfolgt. Informationen hierzu erhalten Sie im Handbuch „Konfiguration“.

Installationsquelle wechseln

Die Installationsquelle ist das Medium, auf dem die zu installierende Software zur Verfügung steht. Sie können von CD (der übliche Weg), von einem Netzwerkserver oder von Festplatte installieren. (Näheres finden Sie in [SuS02b] im Kapitel *YaST2 – Konfigurationen* → *Software* und im ausführlichen YaST2-Hilfetext).

YaST Online Update (YOU)

Das YaST-Online-Update ermöglicht die Installation von wichtigen Upgrades bzw. Verbesserungen. Auf dem SuSE-FTP-Server werden die entsprechenden „Patches“ zum Herunterladen bereitgelegt. Die Installation der aktuellen Pakete kann vollautomatisch erfolgen. Mit 'Manuelles Update' haben Sie jedoch auch die Möglichkeit, selbst zu bestimmen, welche Patches in Ihr SuSE Linux System eingespielt werden.

Mit 'Weiter' laden Sie die Liste aller verfügbaren Patches (falls Sie 'Manuelles Update' gewählt haben) herunter. Nun startet das Modul zur Softwareinstallation (s. *Software installieren/löschen* auf Seite 69), in dem die heruntergeladenen Patches aufgelistet werden. Hier können Sie nun Ihre Auswahl treffen, welche Pakete installiert werden sollen. Sie können auch einfach den Vorschlag der zum Installieren schon gekennzeichneten Patches übernehmen. Sie werden dann wie normale Pakete installiert.

Online-Update von der Konsole

Für Systemadministratoren gibt es auch die Möglichkeit, das Online-Update über eine Shell aufzurufen. Als `root` laden Sie sich mit dem Kommando

```
erde:/root #  yast2 online_update .auto.get
```

die aktuelle Patchliste und alle zutreffenden rpms vom ersten Server in der Liste `/etc/suseservers`. Wenn Sie nur bestimmte Patches laden wollen, können Sie dem Aufruf zusätzlich Optionen mitgeben.

Mögliche Optionen sind `security`, `recommended`, `document`, `YaST2` und `optional`. `security` holt nur sicherheitsrelevante Patches, `recommended`

holt die von SuSE empfohlenen Updates, `document` liefert Ihnen Mitteilungen zu den Patches oder zum FTP-Server, `YaST2` holt nur YaST2-Patches und `optional` liefert Updates von untergeordneter Wichtigkeit.

Die Mitteilungen zu den Patches werden in `/var/lib/YaST/patches/i386/update/X.Y/patches` gespeichert. Sie können sie nur als `root` lesen. `X.Y` ist die jeweilige Version von SuSE Linux.

Der Aufruf zum Download der Security-Patches lautet dann:

```
erde:/root #  yast2 online_update .auto.get security
```

Jedes Mal, wenn Sie `.auto.get` aufrufen, wird normalerweise die Liste der FTP-Server nach `/etc/suseservers` geladen. Wenn Sie das abstellen wollen, müssen Sie die Funktion in der Datei `/etc/rc.config` deaktivieren. Dazu setzen Sie in der Zeile

```
YAST2_LOADFTPSERVER="yes"
```

`yes` auf `no`. Installieren können Sie die Patches nun mit

```
erde:/root #  yast2 online_update .auto.install
```

Dieser Aufruf installiert alle geholten Patches. Wollen Sie nur eine Gruppe installieren, können Sie die gleichen Optionen verwenden wie bei `.auto.get`.

Diese Methode hat den Vorteil, dass sie sich automatisieren lässt. Der Systemadministrator hat die Möglichkeit, sich die Pakete z. B. über Nacht herunterzuladen und morgens die, die er benötigt, zu installieren.

Patch-CD-Update

Im Gegensatz zum Online-Update werden hier die Patches nicht vom ftp-Server geholt, sondern von CD eingespielt (die CD erhalten Kunden des „SuSE Linux Enterprise Servers“). Der Vorteil ist, dass das Einspielen der Patche von CD wenig Zeit in Anspruch nimmt.

Wenn die Patch-CD eingelegt ist, werden in der Maske dieses YaST2-Moduls alle Patches, die sich auf der CD befinden, eingelesen und angezeigt. Aus der Patch-Liste können Sie auswählen, welche installiert werden sollen. Falls Sie vergessen haben sollten, die CD in das Laufwerk zu legen, erscheint eine entsprechende Meldung. Legen Sie dann die CD ein und starten Sie das Patch-CD-Update neu.

Software installieren/löschen

Dieses Modul ermöglicht es, Software auf Ihrem Rechner zu installieren, zu aktualisieren oder zu deinstallieren. Es wurde für SuSE Linux 8.1 komplett überarbeitet und bietet nun mehr Funktionalität und Flexibilität. Die detaillierte Beschreibung des Moduls finden Sie in [SuS02b] im Kapitel *YaST2 – Konfigurationen → Software*.

Update des Systems

Dieses Modul ermöglicht es, Ihr System auf den aktuellen Stand zu bringen. Es werden mehrere Arbeitsschritte aufgerufen und YaST2 wird ermitteln, welche Pakete zu erneuern sind. Falls gewünscht, können Sie für jedes Paket einzeln entscheiden, ob ein Update erfolgen soll. Das Basissystem kann damit allerdings nicht erneuert werden, denn dazu muss vom Installationsmedium, z. B. von CD, gebootet werden. Näheres dazu finden Sie im Kapitel *Update des Systems und Paketverwaltung* auf Seite 33.

Hardware

Neue Hardware muss zunächst entsprechend den Vorgaben des Herstellers eingebaut bzw. angeschlossen werden. Schalten Sie externe Geräte wie Drucker oder Modem an und rufen Sie das entsprechende YaST2-Modul auf. Ein Großteil der handelsüblichen Geräte wird von YaST2 automatisch erkannt, dann zeigt es die technischen Daten an. Falls die automatische Erkennung fehlschlägt, bietet YaST2 eine Geräteliste an (z. B. Modell/Hersteller), aus der Sie sich das passende Gerät auswählen.

Unter 'Hardware' finden Sie Konfigurations-Tools zur Einrichtung diverser Geräte. Der Hardware-Info können Sie die Daten zu Ihrer von YaST2 automatisch erkannten Hardware entnehmen. Das ist unter anderem für Support-Anfragen hilfreich.

In diesem Buch wird nur auf einige der Konfigurations-Tools genauer eingegangen. Eine Beschreibung aller verfügbaren Module zur Hardware-Konfiguration finden Sie in [SuS02b].

Drucker

Mit diesem Modul können Sie die an Ihrem System angeschlossenen Drucker konfigurieren. Es werden lokale als auch Netzwerkdrucker unterstützt. Näheres hierzu finden Sie im Kapitel **??** auf Seite ??.

Anzeige und Eingabegeräte (SaX2)

Dieses Modul übernimmt die Konfiguration der graphischen Oberfläche X11, also die Einstellungen zu Blidschirm(en) und Grafikkarte(n) inklusive Multihead. Sie können dieses Modul auch verwenden, um die Konfiguration (z. B. die Auflösung und Farbtiefe) von X11 nachträglich zu ändern. Kapitel **??** auf Seite ?? gibt Ihnen alle nötigen Details. Außerdem können Sie mit SaX2 Ihre Eingabegeräte einrichten, also Maus, Tastatur, Touchscreen oder Grafiktablets. Die Beschreibung der Bedienung des Moduls finden Sie in [SuS02b] im Abschnitt *YaST2 – Konfigurationen → Anzeige und Eingabegeräte (SaX2)*.

Netzwerk/Basis

Unter 'Netzwerk/Basis' hält YaST2 für Sie grundlegende Konfigurationswerkzeuge bereit, die Ihnen den Weg in das Internet ebnen: die Konfiguration von ADSL, T-DSL in Deutschland, Netzwerkkarte, ISDN, Modem und Hostname und DNS. Die Dokumentationen hierfür finden Sie in [SuS02b].

E-Mail

Das Konfigurationsmodul für die Maileinstellungen wurde aktuellen Anforderungen angepasst. Es wird neben sendmail auch postfix zum Senden von Mails unterstützt. Im Konfigurationsdialog, der sich unter 'Netzwerk/Erweitert' befindet, wählen Sie im ersten Dialog Ihren Verbindungstyp aus:

'Rechner mit permanenter Netzverbindung' Hierbei handelt es sich um eine so genannte „Standleitung", wie sie häufig in Firmen oder sonstigen Institutionen, die viel mit dem Internet arbeiten, zu finden ist. Die Verbindung zum Internet steht permanent, es ist also keine Einwahl nötig. Dieser Menüpunkt gilt jedoch auch für Mitglieder eines lokalen Netzwerks, in dem es keine permanente Internet-Verbindung gibt, jedoch ein zentraler Mailserver zum E-Mail-Versand verwendet wird.

'Rechner mit temporärer Netzverbindung (Modem oder ISDN)' Dies betrifft die meisten Benutzer, die zuhause einen Rechner haben, der keinem Netzwerk angehört, die aber gelegentlich in das Internet gehen – per Einwahl über das Modem, T-DSL/ADSL oder ISDN.

'Keine Netzverbindung' Wenn Sie keinen Internetzugang haben und auch keinem Netz angehören, können Sie natürlich keine E-Mails verschicken oder empfangen.

In weiteren Schritten müssen Sie Ihren Provider für ausgehende Mails wählen und mindestens einen lokalen Benutzer anlegen. Wenn Sie eine „dial–up“-Verbindung haben, können Sie verschiedene POP–Server für unterschiedliche Benutzer für den Mailempfang angeben.

Optional können Sie zusätzlich Aliasnamen festlegen, Adressmaskierungen einstellen oder virtuelle Domänen anlegen. Mit 'Beenden' schließen Sie die Konfiguration ab.

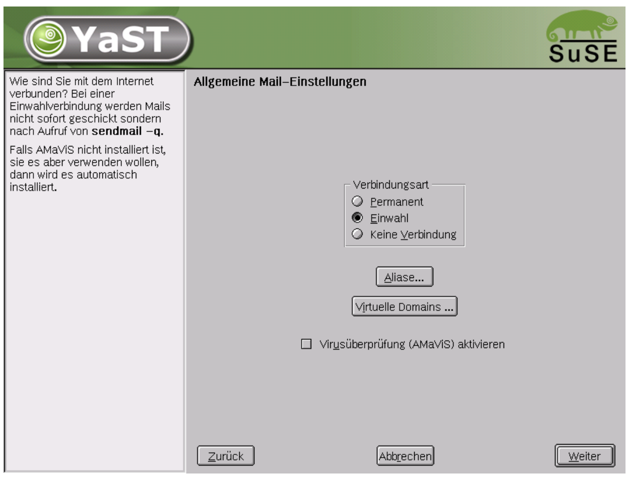


Abbildung 4.2: *Mailkonfiguration*

Netzwerk/Erweitert

Für fortgeschrittenere Internet-Benutzer oder Netzwerk-Betreiber gibt es die Module für Start oder Stopp von Systemdiensten (inetd), Sendmail (mit Experten-Konfiguration), NFS-Client und -Server, Routing, Netzwerk für Experten und NIS-Client. Bei 'Netzwerk für Experten' handelt es sich um die gleiche Funktionalität wie bei 'Konfiguration der Netzwerkkarte' unter 'Netzwerk/Basis', jedoch können Sie hier zusätzlich Modem und ISDN einrichten.

Detaillierte Informationen zum Thema Netzwerk und allem, was dazugehört, finden Sie in den ausführlichen Netzwerk-Kapiteln in diesem Handbuch.

NFS-Server einrichten

Mit YaST2 können Sie sehr schnell einen Rechner Ihres Netzwerks zu einem NFS-Server machen. Das ist ein Server, der Verzeichnisse und Dateien für alle Rechner, denen Sie Zugang gewähren, bereitstellt. Viele Anwendungsprogramme können so z. B. für Mitarbeiter zur Verfügung gestellt werden, ohne dass sie lokal auf deren Rechnern installiert werden müssen.

Details zur Konfiguration des Systems als NFS-Server finden Sie in Abschnitt *NFS – verteilte Dateisysteme* auf Seite 312.

NIS konfigurieren

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen wollen, muss sichergestellt sein, dass Benutzer- und Gruppenkennungen auf allen Rechnern miteinander harmonieren. Das Netzwerk soll für den Anwender transparent sein. Egal welcher Rechner, der Anwender findet immer die gleiche Umgebung vor.

Lesen Sie in Abschnitt *NIS – Network Information Service* auf Seite 307, wie Sie NIS sowohl auf einem Client, als auch als Server konfigurieren.

Hostname und DNS konfigurieren

Hier werden der Hostname und die DNS-Daten des Systems eingestellt. Die nachträgliche Änderung dieser Informationen sollte vermieden werden, da diese Parameter für einen ordnungsgemäßen Netzwerkbetrieb notwendig sind. Bitte lesen Sie in den Kapiteln *Die Einbindung ins Netzwerk* auf Seite 284 und *DNS – Domain Name Service* auf Seite 297 weiter.

Routing konfigurieren

Das Routing stellt ebenfalls einen wichtigen Parameter zur Netzwerkkonfiguration dar. In Kapitel *Die Einbindung ins Netzwerk* auf Seite 284 finden Sie genaue Erläuterungen zum Routing unter Linux.

Sicherheit und Benutzer

YaST2 bietet hier Werkzeuge für eine komfortable Benutzer- und Gruppenverwaltung. Das Konfigurationsmodul 'Systemsicherheit' hält verschiedene vorkonfigurierte Level und eine Möglichkeit für Experten-Einstellungen bereit.

Eine detaillierte Beschreibung des Moduls finden Sie in [SuS02b] im Kapitel *YaST2 – Konfigurationen → Sicherheit und Benutzer*.

Firewall

Mit diesem Modul können Sie sehr einfach die SuSE Firewall 2 einschalten und konfigurieren. Wenn Sie mit dem Internet verbunden sind, sollten Sie unbedingt abgesichert sein, da heute die Angriffsmöglichkeiten enorm sind und die SuSE Firewall sicheren Schutz bietet. Ausführliche Hintergrundinformationen zu Masquerading, Firewalls und zur SuSE Firewall finden Sie im Abschnitt **??** auf Seite ??. Eine Beschreibung des Moduls finden Sie im *Benutzerhandbuch* im Abschnitt *YaST2 – Konfigurationen → Sicherheit und Benutzer*.

System

Unter 'System' haben Sie nochmals die Möglichkeit, den Boot-Modus zu konfigurieren, eine Boot- oder Moduldiskette zu erzeugen, oder die Sprache und Zeitzone einzustellen. Hier finden Sie ebenfalls Module zur Datensicherung und -Restauration. Mit dem Profilmanager können Sie komplette individuelle Systemkonfigurationen anlegen und schnell zwischen diesen wechseln. in [SuS02b] finden Sie die notwendigen Informationen zur Bedienung der einzelnen Module dieser Gruppe. Sysconfig- und Runlevel-Editor sowie der LVM-Partitionierer werden im folgenden kurz beschrieben. Ausführliche Hintergrundinformationen zu den Themen Partionierung, Bootloader und Profilmanager (SCPM) finden Sie in den Abschnitten:

- *Partitionieren für Fortgeschrittene* auf Seite 26
- *Booten und Bootmanager* auf Seite 85
- *SCPM – System Configuration Profile Management* auf Seite 164

Eine einfache Anleitung zum Partitionieren finden Sie zudem in [SuS02b] im Abschnitt *Benutzerdefinierte Installation → Partitionierung*.

LVM

Mit diesem Profi-Partitioniertool haben Sie die Möglichkeit, bestehende Partitionen zu bearbeiten, zu löschen oder neue anzulegen. Von hier aus gelangen Sie zur Soft-RAID- und LVM-Konfiguration .

Hinweis

Viele Hintergrundinformationen und Tipps zum Partitionieren finden Sie im Kapitel *Partitionieren für Fortgeschrittene* auf Seite 26.

Hinweis

Im Normalfall werden die Partitionen während der Installation festgelegt. Wenn Sie jedoch aus Platzgründen eine zweite Festplatte einbauen wollen, so können Sie diese auch im bestehenden Linux-System integrieren. Hierzu ist die neue Festplatte zunächst zu partitionieren und dann müssen diese Partitionen gemountet und in die `/etc/fstab` eingetragen werden. Gegebenenfalls ist es nötig, einige Daten umzukopieren, um eine zu kleine `/opt`-Partition von der alten Festplatte auf die neue zu verschieben.

Wenn Sie die Festplatte, mit der Sie gerade arbeiten, umpartitionieren wollen, ist Vorsicht geboten – grundsätzlich ist dies möglich, danach muss das System aber sofort neu gebootet werden. Unbedenklicher ist es, von der CD zu booten und dann die Umpartitionierung vorzunehmen.

Hinter dem Button 'Experten...' im Partitionierer befindet sich ein Popup-Menü mit folgenden Befehlen:

Partitionstabelle neu einlesen Dient dazu, die Partitionierung neu von der Platte einzulesen. Dies benötigen Sie z. B., wenn Sie die Partitionierung auf der Textkonsole manuell vorgenommen haben.

Mountpunkte von bestehender /etc/fstab übernehmen Dies ist nur während der Installation relevant. Das Einlesen der alten `fstab` nützt, wenn Sie Ihr System nicht updaten, sondern neu installieren. Dann brauchen Sie die Mountpunkte nicht per Hand eingeben.

Partitionstabelle und Disk-Label löschen Hiermit überschreiben Sie den alten Partitiontable komplett. Das kann z. B. hilfreich sein, falls Sie Probleme mit ungewöhnlichen Plattenlabels haben sollten. Mit dieser Methode gehen allerdings alle Daten auf der Festplatte verloren.

Logical Volume Manager (LVM)

Der Logical Volume Manager (LVM) ermöglicht Ihnen eine flexible Verteilung des Festplattenplatzes auf die verschiedenen Filesysteme. Da die Partitionen in einem laufenden System nur mit relativ großem Aufwand geändert werden können, wurde der LVM entwickelt: Er stellt einen virtuellen „Pool" (Volume Group – kurz VG) an Speicherplatz zur Verfügung, aus dem logische

Volumes (LV) nach Bedarf erzeugt werden. Das Betriebssystem greift dann auf diese zu, statt auf die physikalischen Partitionen.

Besonderheiten:

- Es können mehrere Festplatten/Partitionen zu einer großen logischen Partition zusammengefügt werden.
- Geht bei einer LV (z. B. `/usr`) der Platz aus, können Sie diese bei geeigneter Konfiguration vergrößern.
- Mit dem LVM können Sie sogar im laufenden System Festplatten oder LVs ergänzen. Voraussetzung ist allerdings „Hot-Swapable“ Hardware, die für solche Eingriffe geeignet ist.

Der Einsatz von LVM lohnt bereits bei umfangreich genutzten Home-PCs oder kleinen Servern. Wenn Sie einen wachsenden Datenbestand haben wie z. B. bei Datenbanken, MP3-Archiven oder Benutzerverzeichnissen etc., dann bietet sich der Logical Volume Manager an. Dann wäre es z. B. möglich, Filesysteme zu haben, die größer sind als eine physikalische Festplatte. Ein weiterer Vorteil des LVM ist, dass bis zu 256 LVs angelegt werden können. Beachten Sie jedoch bitte, dass sich die Arbeit mit dem LVM sehr von der mit konventionellen Partitionen unterscheidet.

Anleitung und weiterführende Informationen zur Konfiguration des „Logical Volume Manager“ (LVM) finden Sie im offiziellen LVM-Howto bzw. in einem SuSE-Dokument:

- `http://www.sistina.com/lvm/Pages/howto.html`
- `http://www.suse.com/us/support/oracle/`

Konfiguration des LVM mit YaST2

Die LVM-Konfiguration von YaST2 wird vorbereitet, indem Sie während der Installation eine LVM-Partition anlegen. Dazu müssen Sie im Vorschlagsbildschirm

auf 'Partitionierung' klicken, im folgenden Screen dann auf 'Verwerfen' oder 'Ändern'. Danach müssen Sie eine Partition für LVM anlegen. Dazu wählen Sie im Partitionierer 'Anlegen' → 'Nicht formatieren' und wählen dort den Punkt '0x8e Linux LVM'. Die weitere Partitionierung mit LVM können Sie direkt im Anschluss oder auch später im installierten System vornehmen, indem Sie im Partitionierer die LVM-Partition markieren und dann afu 'LVM...' klicken.

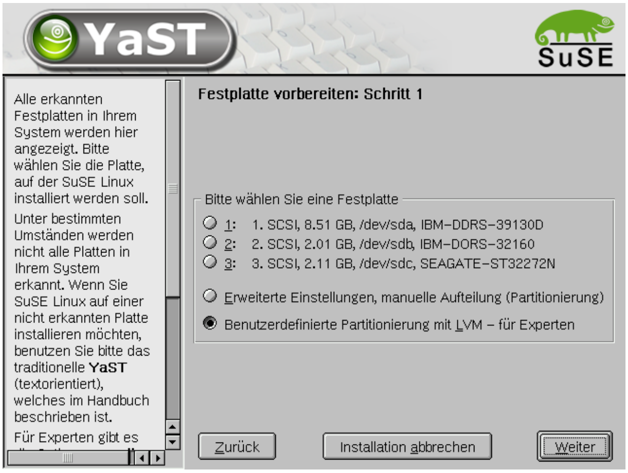


Abbildung 4.3: *YaST2: LVM während der Installation aktivieren*

LVM – Partitionierer

Nachdem Sie im Partitionieren 'LVM...' gewählt haben, sehen Sie als erstes kommen Sie in einen Dialog, in dem Sie die Partitionierung Ihrer Festplatten ändern können. Hier können Sie bestehende Partitionen löschen, existierende Partitionen ändern und neue anlegen. Eine Partition, die für LVM verwendet werden soll, muss die Partitionskennung 8E haben. Diese Partitionen sind mit dem Text „Linux LVM" in der Partitionsliste des Fensters versehen (s. letzter Abschnitt).

Es ist nicht nötig, alle Partitionen, die für LVM vorgesehen sind, einzeln auf die Partitionskennung 8E zu setzen. YaST2 setzt die Partitionskennung einer Partition, die einer LVM Volume Group zugeordnet wird, automatisch auf 8E wenn dies nötig ist. Wenn auf Ihren Platten unpartitionierte Bereiche vorhanden sind, sollten Sie in diesem Dialog für alle diese Bereiche LVM-Partitionen anlegen. Diese Partitionen sollten Sie gleich auf die Partitionskennung 8E setzen. Diese müssen nicht formatiert werden und es kann für sie kein Mountpunkt eingetragen werden.

Falls auf Ihrem System bereits eine gültige LVM-Konfiguration existiert, wird diese bei Beginn der LVM-Konfiguration automatisch aktiviert. Ist diese Aktivierung erfolgt, kann die Partitionierung aller Platten, die eine Partition enthalten, die zu einer aktivierten Volume Group gehört, nicht mehr verändert werden. Der Linux-Kernel weigert sich, die veränderte Partitionierung einer Festplatte einzulesen, solange auch nur eine Partition dieser Platte benutzt

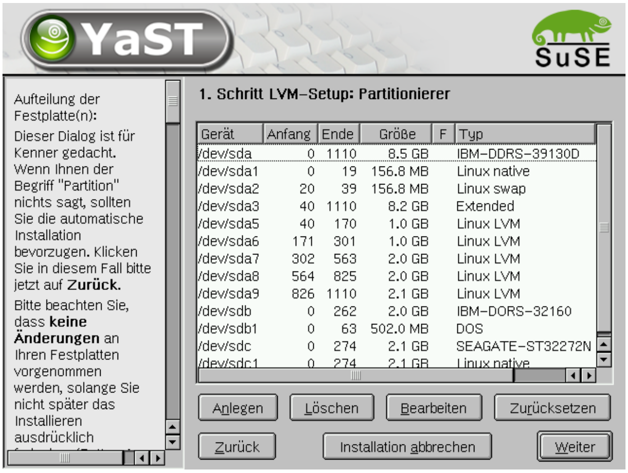


Abbildung 4.4: *YaST2: LVM-Partitionierer*

wird.

Eine Umpartitionierung von Platten, die nicht zu einer LVM Volume Group gehören, ist natürlich problemlos möglich. Falls Sie bereits eine gültige LVM-Konfiguration auf Ihrem System haben, ist ein Umpartitionieren normalerweise nicht erforderlich. In dieser Maske müssen Sie nun alle Mountpoints konfigurieren, die nicht auf LVM Logical Volumes liegen. Zumindest das Root-Filesystem muss in YaST2 auf einer normalen Partition liegen. Wählen Sie diese Partition aus der Liste aus und legen Sie diese mit dem Button 'Bearbeiten' als Root-Filesystem fest.

Wir empfehlen aufgrund der größeren Flexibilität von LVM, alle weiteren Filesysteme auf LVM Logical Volumes zu legen. Nach Festlegen der Root-Partition können sie diesen Dialog verlassen.

LVM – Einrichtung der Physical Volumes

In diesem Dialog werden die LVM Volume Groups (oft mit „VG" abgekürzt) verwaltet. Wenn auf Ihrem System noch keine Volume Group existiert, werden Sie in einem Popup-Fenster aufgefordert, eine anzulegen. Als Name für die Volume Group auf der sich die Dateien des SuSE Linux Systems befinden, wird „system" vorgeschlagen.

Die so genannte Physical Extent Size (oft abgekürzt mit PE-Size) bestimmt die maximale Größe eines Physical und Logical Volumes in dieser Volume Group.

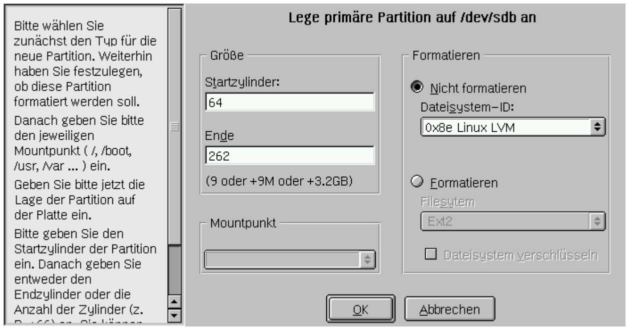


Abbildung 4.5: YaST2: *LVM-Partition anlegen*

Dieser Wert wird normalerweise auf 4 Megabyte festgelegt. Dies lässt eine Maximalgröße für ein Physical und Logical Volume von 256 Gigabyte zu. Sie sollten die Physical Extent Size also nur dann erhöhen (z. B. auf 8, 16 oder 32 Megabyte), wenn Sie größere Logical Volumes als 256 Gigabyte benötigen.

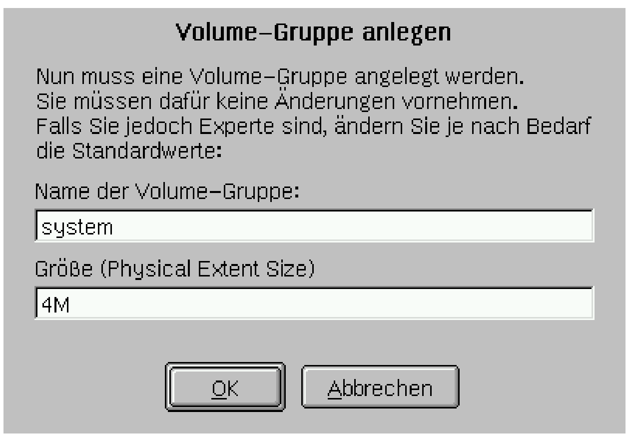


Abbildung 4.6: YaST2: *Volume Group anlegen*

In dem folgenden Dialog sind alle Partitionen aufgelistet, die entweder den Type "Linux LVM" oder "Linux native" haben. Alle Swap- und DOS-Partitionen werden also nicht angezeigt. Wenn eine Partition bereits einer Volume Group zugeordnet ist, wird der Name der Volume Group in der Liste angezeigt. Nicht zugeordnete Partitionen enthalten die Kennung "–".

Die gegenwärtig bearbeitete Volume Group kann in der Auswahlbox links oben geändert werden. Mit den Buttons rechts oben ist es möglich, zusätzliche Volume Groups anzulegen und bestehende VGs zu löschen. Es können allerdings nur solche Volume Groups gelöscht werden, denen keine Partitionen mehr zugeordnet sind. Für ein normal installiertes SuSE Linux System ist es nicht nötig, mehr als eine Volume Group anzulegen. Eine Partition, die einer Volume Group zugeordnet ist, wird auch Physical Volume (oft mit PV abgekürzt) genannt.

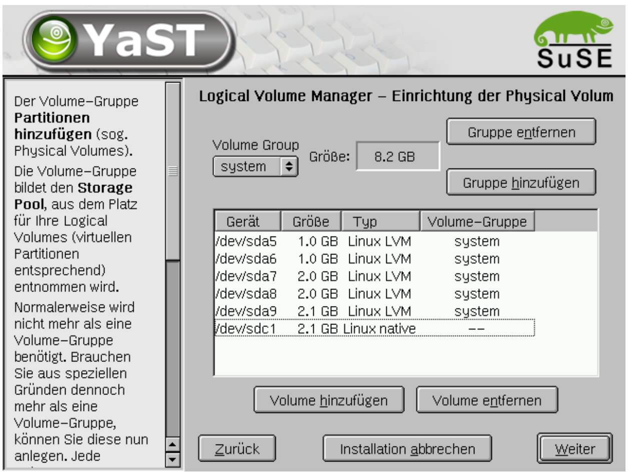


Abbildung 4.7: *YaST2: Übersicht über die Partitionen*

Um eine bisher nicht zugeordnete Partition der angewählten Volume Group hinzuzufügen, wählen Sie zuerst die Partition an und aktivieren dann den Button 'Volume hinzufügen' unterhalb der Auswahlliste. Daraufhin wird der Name der Volume Group bei der angewählten Partition eingetragen. Sie sollten alle Partitionen, die Sie für LVM vorgesehen haben, einer Volume Group zuordnen, sonst bleibt der Platz auf der Partition ungenutzt. Bevor Sie den Dialog verlassen können, muss jeder Volume Group mindestens eine Physical Volume zugeordnet sein.

Logical Volumes

Im diesem Dialog werden die Logical Volumes (oft einfach mit „LV" abgekürzt) verwaltet.

Logical Volumes sind jeweils einer Volume Group zugeordnet und haben eine bestimmte Größe. Normalerweise wird auf einem Logical Volume ein Filesys-

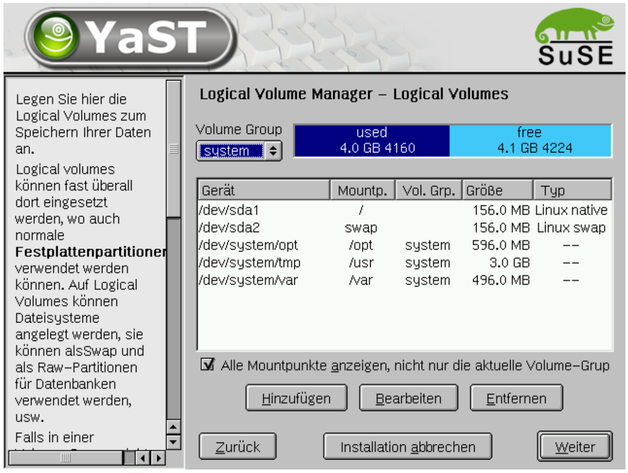


***Abbildung 4.8:** YaST2: Verwaltung der Logical Volumes*

tem (z. B. reiserfs, ext2) angelegt und ihm wird ein Mountpunkt zugeordnet. Unter diesem Mountpunkt sind dann im installierten System die Dateien zu finden, die auf diesem Logical Volume gespeichert sind. In der Liste sind alle normalen Linux-Partitionen, denen ein Mountpunkt zugeordnet ist, alle Swap-Partitionen und alle bereits existierenden Logical Volumes eingetragen.

Wenn Sie bereits vorher auf Ihrem System LVM konfiguriert hatten, sind die existierenden Logical Volumes bereits hier eingetragen. Sie müssen diesen Logical Volumes allerdings noch den passenden Mountpunkt zuordnen. Wenn Sie zum ersten mal auf einem System LVM konfigurieren, dann existieren in dieser Maske noch keine Logical Volumes und Sie müssen für jeden Mountpunkt ein Logical Volume erzeugen (mit dem Button 'Hinzufügen'), die Größe, den Filesystem-Typ (z. B. reiserfs oder ext2) und den Mountpunkt (z. B. `/var`, `/usr`, `/home`) festlegen.

Wenn Sie mehrere Volume Groups angelegt haben, können Sie in der Auswahlliste links oben zwischen den einzelnen Volume Groups wechseln. Die angelegten Logical Volumes liegen jeweils in der links oben anzeigten Volume Group. Haben Sie alle Logical Volumes so angelegt, wie sie benötigt werden, dann ist die LVM-Konfiguration beendet. Sie können den Dialog verlassen und mit der Software-Auswahl fortfahren, falls Sie sich im Installations-Prozess befinden.

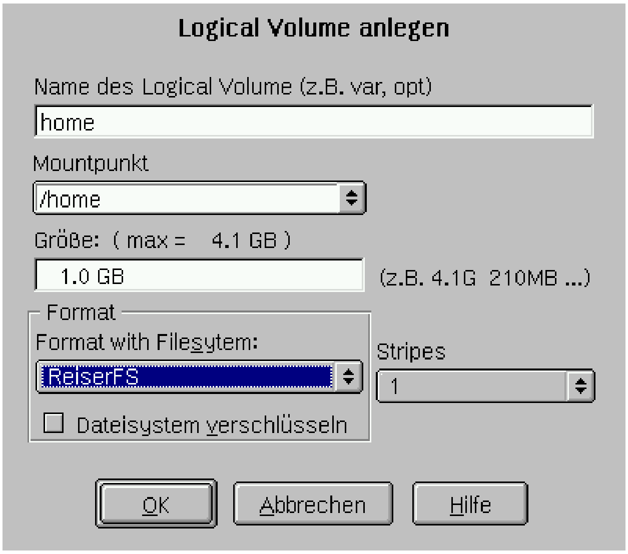


Abbildung 4.9: *YaST2: Logical Volumes anlegen*

Achtung

Der Einsatz des LVM ist auch mit erhöhten Risiken wie z. B. Datenverlust verbunden. Mögliche Gefahren sind Programmabstürze, Stromausfälle oder fehlerhafte Kommandos.

Sichern Sie bitte Ihre Daten bevor Sie LVM einsetzen oder Volumes umkonfigurieren – arbeiten Sie also nie ohne Backup!

Achtung

Soft-RAID

Der Sinn von RAID (engl. *Redundant Array of Inexpensive Disks*) ist, mehrere Festplattenpartitionen zu einer großen „virtuellen" Festplatte zu vereinen, um die Performance und die Datensicherheit zu optimieren. Dabei geht das eine jedoch auf Kosten des anderen. Der so genannte „RAID-Level" definiert den Zusammenschluss und die gemeinsame Ansteuerung der Festplatten, die von einem RAID-Controller vorgenommen wird.

Ein RAID-Controller verwendet meist das SCSI-Protokoll, da es gegenüber dem IDE-Protokoll mehr Festplatten besser ansteuern kann und besser für

eine parallele Abarbeitung der Befehle geeignet ist.

Statt eines RAID-Controllers, der unter Umständen sehr teuer sein kann, ist auch Soft-RAID in der Lage, diese Aufgaben zu übernehmen. SuSE Linux bietet Ihnen die Möglichkeit, mit Hilfe von YaST2 mehrere Festplatten zu einem Soft-RAID-System zu vereinen – eine sehr günstige Alternative zu Hardware-RAID.

Gängige RAID-Level

RAID 0 Dieser Level verbessert die Performance Ihres Datenzugriffs. Im Grunde ist dies gar kein RAID, da es keine Datensicherung gibt, doch die Bezeichnung „RAID 0" hat sich für diese Art von System eingebürgert. Bei RAID 0 schließt man mindestens zwei Festplatten zusammen. Die Performance ist sehr gut – jedoch ist das RAID-System zerstört und Ihre Daten sind verloren, wenn auch nur eine von noch so vielen Festplatten ausfällt.

RAID 1 Dieser Level bietet eine äußerst zufrieden stellende Sicherheit für die Daten, weil diese 1:1 auf eine andere Festplatte kopiert werden. Dies nennt man „Festplattenspiegelung" – ist eine Platte zerstört, liegt eine Kopie deren Inhalts auf einer anderen. Es dürfen alle bis auf eine der Festplatten fehlerhaft sein, ohne Daten verloren zu haben. Die Schreibperformance leidet durch den Kopiervorgang ein wenig bei einer Verwendung von RAID 1 (10-20 % langsamer), dafür geht der Lesezugriff deutlich schneller im Vergleich zu einer einzelnen normalen physikalischen Festplatte, weil die Daten doppelt vorhanden sind und somit parallel ausgelesen werden können.

RAID 5 RAID 5 ist ein optimierter Kompromiss aus den beiden anderen Levels was Performance und Redundanz betrifft. Das Festplattenpotential entspricht der Anzahl der eingesetzten Platten minus einer. Die Daten werden wie bei RAID 0 über die Festplatten verteilt. Für die Sicherheit sorgen die „Paritätsblöcke", die bei RAID 5 auf einer der Partitionen angelegt werden. Diese werden mit XOR miteinander verknüpft – somit lässt sich beim Ausfall einer Partition durch den dazugehörigen Paritätsblock der Inhalt nach XOR rekonstruieren. Bei RAID 5 ist zu beachten, dass nicht mehr als eine Festplatte gleichzeitig ausfallen darf. Ist eine zerstört, muss sie schnellstmöglichst ausgetauscht werden, damit die Daten nicht verloren gehen.

Soft-RAID-Konfiguration mit YaST2

Zur Soft-RAID-Konfiguration gelangen Sie entweder über ein eigenes 'RAID'-Modul unter 'System' oder über das Partitionierungs-Modul unter 'Hardwa-

re'.

1. Schritt: Partitionieren

Zunächst sehen Sie unter 'Experten-Einstellungen' im Partitionierungs-Tool Ihre Partitionen aufgelistet. Wenn Sie bereits Soft-RAID-Partitionen angelegt haben, erscheinen diese hier. Andernfalls müssen Sie neue anlegen. Bei RAID 0 und RAID 1 benötigen Sie mindestens zwei Partitionen – bei RAID 1 sind das im Normalfall genau zwei. Für eine Verwendung von RAID 5 hingegen sind mindestens drei Partitionen nötig. Es ist zu empfehlen, nur Partitionen gleicher Größe zu nehmen.

Die einzelnen Partitionen eines RAIDs sollten auf verschiedenen Festplatten liegen, damit das Risiko eines Datenverlustes durch den Defekt einer Festplatte bei RAID 1 und 5 verhindert wird bzw. die Performance bei RAID 0 optimiert wird.

2. Schritt: RAID anlegen

Wenn Sie auf 'RAID' klicken, erscheint der Dialog, in dem Sie den RAID-Level 0, 1 oder 5 auswählen. In der nächsten Maske haben Sie die Möglichkeit, die Partitionen dem neuen RAID zuzuordnen. Hinter 'Experten-Optionen' finden Sie Einstellmöglichkeiten für die „chunk-size“ – hier können Sie Fein-Tuning für die Performance vornehmen. Die Aktivierung der Checkbox 'Persistent superblock' sorgt dafür, dass RAID-Partitionen gleich beim Booten als solche erkannt werden.

Nach Beendigung der Konfiguration sehen Sie auf der Experten-Seite im Partitionierungs-Modul dann das Device `/dev/md0` (etc.) als „RAID“ gekennzeichnet.

Troubleshooting

Ob eine RAID-Partition zerstört ist, können Sie dem Inhalt der Datei `/proc/mdstats` entnehmen. Grundsätzliche Vorgehensweise in einem Fehlerfall ist es, Ihr Linux-System herunterzufahren und die defekte Festplatte durch eine neue gleichartig partitionierte zu ersetzen. Dann starten Sie Ihr System neu und verwenden den Befehl `raidhotadd /dev/mdX /dev/sdX`. Damit wird die neue Festplatte automatisch in das RAID-System integriert und vollautomatisch rekonstruiert.

Eine Anleitung zur Konfiguration von Soft-RAID und weitere Details hierzu finden Sie im angegebenen Howto:

- `/usr/share/doc/packages/raidtools/Software-RAID-HOWTO.html`
- `http://www.LinuxDoc.org/HOWTO/Software-RAID-HOWTO.html`

oder in der Linux-RAID-Mailingliste z. B. über:

- `http://www.mail-archive.com/linux-raid@vger.rutgers.edu`

Dort finden Sie auch Hilfe, falls wider Erwarten komplexe Probleme auftreten sollten.

Runlevel-Editor

Der Runlevel des Systems, der sog. „Betriebsmodus“, wird nach dem Booten Ihres Systems hochgefahren. Bei SuSE Linux ist dies üblicherweise Runlevel 5 (voller Multiuserbetrieb mit Netzwerk und KDM, dem grafischen Login). Mit diesem Modul lässt sich erstens der Standard-Runlevel verändern und zweitens können Sie einstellen; vgl. Tabelle 11.1 auf Seite 228, welche Dienste in welchem Runlevel jeweils gestartet werden..

Die Hintergründe zu den Runleveln und eine genauere Beschreibung des Runlevel-Editors unter Linux sind in Abschnitt *Die Runlevels* ff. erläutert.

Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig` sind die Dateien mit den wichtigsten Einstellungen für SuSE Linux hinterlegt (ehemals in der Datei `/etc/rc.config` zentral verwaltet). Der Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und anschließend in die einzelnen Konfigurationsdateien übernommen werden.

Im Abschnitt *SuSEconfig, /etc/sysconfig und /etc/rc.config* auf Seite 233 ff. finden Sie detaillierte Informationen über den Sysconfig-Editor sowie über die Sysconfig-Variablen.

Sonstiges

Unter 'Sonstiges' haben Sie die Möglichkeit, Treiber-CDs des Herstellers zu laden und das Startprotokoll (`/var/log/boot.msg`) bzw. das Systemprotokoll (`/var/log/messsages`) anzeigen zu lassen. Außerdem können Sie mit einem Modul eine Anfrage an den Installationssupport stellen.

Die Module sind wieder in [SuS02b] genauer beschrieben.

5 Booten und Bootmanager

Im Folgenden werden verschiedene Methoden vorgestellt, wie sich das fertig installierte System booten lässt. Um das Verständnis der einzelnen Methoden zu erleichtern, werden zunächst einige technische Details des Bootprozesses erläutert. Dann wird ausführlich der Bootmanager LILO erklärt und anschließend im Vergleich dazu GRUB. Etwas knapper wird loadlin vorgestellt.

LILO wurde bisher als Standard-Bootloader verwendet. Wenn Sie ein Update von einer früheren Version durchführen, wird auch wieder LILO eingerichtet. Bei einer Neuinstallation wird dagegen GRUB verwendet.

Der Bootvorgang auf dem PC 86
Bootkonzepte 87
Map Files, LILO und GRUB 88
LILO im Überblick 89
LILO nach Maß 92
Installation und Deinstallation von LILO 100
Beispielkonfigurationen 104
Probleme mit LILO 107
Booten mit GRUB 107
Einrichten des Bootmechanismus mit loadlin 110
Für alle Fälle: Boot-CD erstellen 117

Der Bootvorgang auf dem PC

Nach dem Einschalten des Rechners werden vom BIOS (engl. *Basic Input Output System*) Bildschirm und Tastatur initialisiert sowie der Hauptspeicher getestet. Bis zu diesem Zeitpunkt verfügt der Rechner über keine Massenspeichermedien.

Nachdem das Rumpfsystem seine „Innenschau" beendet hat, kann es sich der Erkundung der übrigen Welt widmen. Informationen über aktuelles Datum, Zeit und eine Auswahl der wichtigsten Peripherie-Geräte werden aus den CMOS-Werten (*CMOS setup*) ausgelesen. Da nun die erste Festplatte einschließlich ihrer Geometrie bekannt sein sollte, kann das Laden des Betriebssystems von dort beginnen.

Dazu wird von der ersten Festplatte der physikalisch erste Datensektor von 512 Byte Größe in den Speicher geladen und die Kontrolle geht auf das Programm zu Beginn dieses Sektors über. Die Abfolge der auf diese Weise ausgeführten Anweisungen bestimmt den weiteren Ablauf des Bootvorgangs. Die ersten 512 Byte auf der ersten Festplatte werden deshalb auch als *Master Boot Record* (MBR) bezeichnet.

Bis zu diesem Zeitpunkt (Laden des MBR) läuft der Bootvorgang völlig unabhängig vom installierten System auf jedem PC immer gleich ab und der Computer hat bis dahin für den Zugriff auf die Peripherie lediglich die im BIOS gespeicherten Routinen (Treiber) zur Verfügung.

Master Boot Record

Die Struktur des MBR ist durch eine betriebssystemübergreifende Konvention festgelegt. Die ersten 446 Byte sind für Programmcode reserviert. Die nächsten 64 Byte bieten Platz für eine Partitionstabelle mit bis zu vier Einträgen; Abschnitt *Partitionieren für Fortgeschrittene* auf Seite 26. Ohne die Partitionstabelle gibt es keine Dateisysteme, d. h. die Festplatte ist praktisch nicht zu verwenden. Die letzten 2 Byte müssen eine feste „magische Zahl" (AA55) enthalten: ein MBR, der dort etwas anderes stehen hat, wird vom BIOS und von allen PC-Betriebssystemen als ungültig angesehen.

Bootsektoren

Bootsektoren sind die jeweils ersten Sektoren der Festplatten-Partitionen, außer bei der erweiterten Partition, die nur ein „Behälter" für andere Partitionen ist. Diese Bootsektoren bieten 512 Byte Platz und sind dazu gedacht,

Code aufzunehmen, der ein auf dieser Partition befindliches Betriebssystem starten kann. Dies gilt für Bootsektoren formatierter DOS-, Windows- oder OS/2-Partitionen, die zusätzlich noch wichtige Grunddaten des Dateisystems enthalten. Im Gegensatz dazu sind Bootsektoren von Linux-Partitionen – auch nach der Anlage eines Dateisystems – von Hause aus erst einmal leer! Eine Linux-Partition ist daher *nicht von selbst startbar,* auch wenn sie einen Kernel und ein gültiges Root-Dateisystem enthält.

Ein Bootsektor mit gültigem Systemstart-Code trägt in den letzten 2 Byte dieselbe „magische" Kennung wie der MBR (AA55).

Booten von DOS oder Windows 95/98

Im DOS-MBR der ersten Festplatte ist ein Partitionseintrag als *aktiv* (engl. *bootable*) gekennzeichnet, was bedeutet, dass dort nach dem zu ladenden System gesucht werden soll. Deshalb muss DOS zwingend auf der ersten Festplatte installiert sein. Der DOS-Programmcode im MBR ist die erste Stufe des Bootloaders (engl. *first stage bootloader*) und überprüft, ob auf der angegebenen Partition ein gültiger Bootsektor vorhanden ist.

Falls dies der Fall ist, kann der Code in diesem Bootsektor als „zweite Stufe" des Bootloaders (engl. *secondary stage loader*) nachgestartet werden. Dieser lädt nun die Systemprogramme, und schließlich erscheint der gewohnte DOS-Prompt bzw. es startet die Windows 95/98-Oberfläche.

Unter DOS lässt sich nur eine einzige primäre Partition als aktiv markieren. Folglich kann das DOS-System nicht auf logischen Laufwerken in einer erweiterten Partition untergebracht werden.

Bootkonzepte

Das einfachste „Bootkonzept" betrifft einen Rechner mit einem einzigen Betriebssystem. Die Abläufe in der Startphase in diesem Fall haben wir soeben geschildert. Ein solcher Bootvorgang ist auch für einen Nur-Linux-Rechner denkbar. Dann kann theoretisch auf die Installation von LILO verzichtet werden, allerdings wäre es so nicht möglich, dem Kernel während des Startens eine Kommandozeile (mit Spezialwünschen zum Startvorgang, zusätzlichen Hardware-Informationen usw.) mitzugeben. Sobald mehr als ein Betriebssystem auf einem Rechner installiert ist, bieten sich verschiedene Bootkonzepte an:

Zusätzliche Systeme von Diskette booten Ein Betriebssystem wird von Platte geladen, mit Hilfe von Boot-Disketten können alternativ weitere Betriebssysteme vom Disketten-Laufwerk aus gestartet werden.

- *Bedingung:* Ein bootfähiges Diskettenlaufwerk ist vorhanden.
- *Beispiel:* Sie installieren Linux zusätzlich zu Ihrem Windows-System und starten Linux stets von Bootdiskette.
- *Vorteil:* Sie ersparen sich die Bootloader-Installation.
- *Nachteile:* Sie müssen *sehr* darauf bedacht sein, einen Sicherheitsvorrat funktionierender Bootdisketten zu haben und der Start dauert länger.
- Dass Ihr Linux ohne Bootdiskette nicht starten kann, mag je nach beabsichtigtem Einsatz Ihres Rechners ein Vor- oder Nachteil sein.

Zusätzliche Systeme zur Laufzeit nachladen Ein bestimmtes Betriebssystem wird bei jedem Systemstart geladen, weitere können von diesem aus optional nachgeladen werden.

- *Bedingung:* Geeignete Programme zum Nachstarten eines Systems sind vorhanden.
- *Beispiele:* Das Laden von Linux von DOS oder Windows aus mit Hilfe des Programms loadlin.exe (vgl. Abschnitt *Einrichten des Bootmechanismus mit loadlin* auf Seite 110) oder das Hochfahren eines NetWare-Servers von DOS aus mit server.exe.

Installation eines Bootmanagers Ein Bootmanager erlaubt, mehrere Systeme gleichzeitig auf einem Rechner zu halten und sie abwechselnd zu nutzen. Der Benutzer wählt das zu ladende System bereits während des Bootvorgangs aus; ein Wechsel erfordert den Neustart des Rechners. Bedingung ist dabei, dass der gewählte Bootmanager mit allen Betriebssystemen „harmoniert".

Map Files, LILO und GRUB

Das größte Problem beim Booten eines Betriebssystems besteht darin, dass der Kernel eine Datei auf einem Dateisystem auf einer Partition auf einer Festplatte ist. Für das BIOS allerdings sind Dateisysteme und Partitionen völlig unbekannte Konzepte.

Um dieses Problem zu umgehen, wurden sogenannte „Maps“ und „Map Files“ eingeführt. In den Maps werden die physikalischen Blöcke auf der Festplatte notiert, die von den logischen Dateien belegt sind. Wenn so eine Map verarbeitet wird, lädt das BIOS die physikalischen Blöcke in der Reihenfolge, wie sie in der Map-Datei angegeben ist, und baut so die logische Datei im Speicher auf.

Der Hauptunterschied zwischen LILO und GRUB besteht nun darin, dass LILO sich fast vollständig auf Maps verläßt, während GRUB versucht, sich so bald als möglich während des Bootens von den festen Maps zu lösen. Dies erreicht GRUB durch *File System Code*, der es ermöglicht, auf Dateien durch die Pfadangabe zuzugreifen und nicht mehr durch die Blocknummern.

Dieser Unterschied hat historische Gründe. In den frühen Tagen von Linux kämpften viele verschieden Dateisysteme um die Vorherrschaft. Werner Almesberger entwickelte einen Bootloader (LILO), der nicht wissen musste, auf welchem Filesystem der zu bootende Kernel angelegt war. Die Idee hinter GRUB geht sogar noch weiter zurück in die Tage des traditionellen Unix und BSD. Diese hatten sich gewöhnlich auf ein Dateisystem festgelegt und am Anfang desselben einen bestimmten Platz für den Bootloader reserviert. Dieser Bootloader kannte die Struktur des Dateisystems, in das er eingebunden war, und fand dort die Kernel mit ihren Namen im root-Verzeichnis.

Ein weiterer fundamentaler Unterschied besteht darin, dass der LILO Bootcode in 16-bit Assembler geschrieben ist, während GRUB weitestgehendst in 32-bit portablem C-Code implementiert ist. Die Auswirkungen zu beschreiben, übersteigt allerdings den Rahmen dieses Buches.

Der folgende Abschnitt beschreibt die Installation und Konfiguration eines Bootmangers am Beispiel des Linux Bootmanagers LILO. Eine vollständige Beschreibung von LILO finden Sie in [Alm96]. Diese Anleitung finden Sie unter: `/usr/share/doc/packages/lilo/user.dvi`. Lesen Sie den Text am Bildschirm mit Programmen wie `xdvi` oder drucken Sie den Text mit dem Befehl: `lpr /usr/share/doc/packages/lilo/user.dvi`

Die Unterschiede bei der Verwendung von GRUB werden im Abschnitt *Booten mit GRUB* auf Seite 107 dargelegt. Im Anschluss finden Sie eine Beschreibung von loadlin.

LILO im Überblick

Der Linux-Bootloader LILO ist für die Installation im MBR geeignet (Einzelheiten später in Abschnitt *Wo kann LILO installiert werden?* auf Seite 91 und in

Abschnitt *Installation und Deinstallation von LILO* auf Seite 100). LILO hat Zugriff auf beide im Real Modus bekannten Festplatten und ist bereits von seiner Installation her in der Lage, alle benötigten Daten auf den „rohen" Festplatten, ohne Informationen zur Partitionierung, zu finden. Deshalb lassen sich auch Betriebssysteme von der zweiten Festplatte booten. Die Einträge in der Partitionstabelle werden im Gegensatz zum DOS-Bootvorgang ignoriert.

Tipp

Von einem „rohen" Datenträger (engl. *raw device*) spricht man, wenn auf ein Blockgerät (Festplatte, Partition, Diskette ...) direkt als einzelne (Geräte-)Datei zugegriffen wird, nicht über ein darauf angelegtes *Dateisystem*.

Tipp

Der Hauptunterschied zum DOS-Bootvorgang besteht jedoch in der Möglichkeit, beim Booten zwischen dem Laden verschiedener installierter Betriebssysteme wählen zu können. Nach dem Laden des MBR in den Speicher wird LILO gestartet; LILO bietet nun dem Benutzer die Auswahl aus einer Liste vorinstallierter Systeme an. Er kann beim Systemstart Bootsektoren von Partitionen laden, um ein Betriebssystem von dieser Partition zu starten, oder den Linux-Kernel laden und Linux starten. Zudem bietet er die wichtige Gelegenheit, dem Linux-Kernel eine Kommandozeile mitzugeben. Zu Sicherheitszwecken können die LILO-Dienste ganz oder teilweise passwortgeschützt werden.

Woraus besteht LILO?

Die LILO-Startmaschinerie umfasst die folgenden Bestandteile:

- *LILO-Bootsektor* mit einem Anfangsstück („erste Stufe") des LILO-Codes, das den eigentlichen LILO beim Systemstart aktiviert.

  Tipp

  Die von LILO installierten Bootsektoren enthalten eine Byte-Sequenz, die auch für Bootsektorviren charakteristisch ist. Daher ist es nicht verwunderlich, wenn DOS-Virenscanner in Dateien wie `/boot/chain.b` oder `/boot/os2_d.b` das AIRCOP-Bootsektor-Virus gefunden zu haben glauben.

  Tipp

- LILO-Maschinencode, standardmäßig in `/boot/boot-menu.b`

- *Map-Datei* (`/boot/map`), in der LILO bei seiner Installation einträgt, wo die Linux-Kernel und sonstigen Daten, die er braucht, zu finden sind.
- optional: die *Message-Datei* `/boot/message`, die standardmäßig eine graphische LILO-Bootauswahl erzeugt.
- die verschiedenen Linux-Kernel und Bootsektoren, die LILO zum Starten anbieten soll.

Achtung

Jeder Schreibzugriff (auch durch Dateiverschiebung) auf einen dieser Bestandteile macht die Map-Datei ungültig und daher eine *Neu--Installation von LILO* erforderlich (siehe auf Seite 101)! Dies betrifft vor allem den Wechsel zu einem neuen Linux-Kernel.

Achtung

Wo kann LILO installiert werden?

Gemeint ist mit dieser Frage der LILO-Bootsektor („erste Stufe"). Bevor wir darauf eingehen, wollen wir aber gleich hier auf eine mögliche Einschränkung hinweisen:

Abhängig von der BIOS-Version Ihres Rechner kann es notwendig sein, *alle* Bestandteile der LILO-Startmaschinerie und das Kernelimage `/boot/vmlinuz` innerhalb der *ersten 1024 Zylinder* zu legen! Dies kann man durch eine kleine Extrapartition erreichen, die unter dem Verzeichnis `/boot` eingehängt („gemountet") wird und die komplett innerhalb der ersten 1024 Zylinder liegt. Nähere Informationen dazu finden Sie in der SuSE Support Datenbank: `http://sdb.suse.de/de/sdb/html/1024_Zylinder.html`

Für den LILO-Bootsektor stehen folgende Installationsziele zur Auswahl:

Auf einer *Diskette* Dies ist die einfachste, aber auch langsamste Methode, mit LILO zu booten (siehe auf Seite ??). Wählen Sie diese Methode, wenn Sie den bestehenden Bootsektor nicht überschreiben wollen.

Im *Bootsektor* einer primären Linux-Partition der ersten Festplatte
Diese Variante lässt den MBR unberührt. Vor dem Booten muss diese Partition mit fdisk als aktiv markiert werden. Rufen Sie dazu als `root` `fdisk -s <Partition>` auf. fdisk fragt Sie nun nach einer Eingabe. `'m'` gibt Ihnen eine Liste der möglichen Eingaben und mit `'a'` können Sie die angegebene Partition startbar machen.

Wenn Linux ganz auf logischen Laufwerken oder Partitionen der zweiten Festplatte eingerichtet wurde, bleibt für LILO nur der Bootsektor der erweiterten Partition der ersten Festplatte – sofern diese existiert – übrig. Linux fdisk kann auch diese Partition aktivieren.

Wenn Sie mehrere Betriebssysteme von der Festplatte booten wollen, ist dieses Verfahren allerdings etwas umständlich: jedes Mal *vor* einem Betriebssystem-Wechsel müssen Sie unter dem bisherigen Betriebssystem dessen Startpartition deaktivieren und die des nächsten Betriebssystem aktivieren. Die folgenden beiden Verfahren sind für diesen Fall besser geeignet.

Im *Master Boot Record* Diese Variante bietet die größte Flexibilität. Insbesondere ist dies die einzige Möglichkeit, Linux von Festplatte aus zu booten, wenn sämtliche Linux-Partitionen auf der zweiten Festplatte liegen, und auf der ersten keine erweiterte Partition zur Verfügung steht. Ein Veränderung des MBR birgt aber bei unsachgemäßer Installation auch gewisse Risiken. Die nötigen Sicherheitsmaßnahmen kommen in Abschnitt *Installation und Deinstallation von LILO* auf Seite 100 zur Sprache.

Wenn Sie bisher einen *anderen Bootmanager* verwendet haben... ...und ihn weiterverwenden wollen, gibt es, je nach dessen Fähigkeiten, noch weitere Möglichkeiten. Ein häufiger Fall: Sie haben eine primäre Linux--Partition auf der zweiten Platte, von der aus Sie Linux starten wollen. Ihr anderer Bootmanager wäre imstande, diese Partition über den Bootsektor zu starten. Dann können Sie diese Partition startbar machen, indem Sie LILO in deren Bootsektor installieren, und sie dem anderen Bootmanager als startbar melden.

Achtung

Vorsicht aber mit dem Wunsch, eine *logische* Linux-Partition startbar zu machen, indem Sie LILO dort installieren: Es geht oft gut; aber selbst wenn Ihr anderer Bootmanager logische Partitionen starten könnte, ist der Erfolg ausdrücklich *nicht garantiert.*

Achtung

LILO nach Maß

Als flexibler Bootmanager bietet LILO zahlreiche Möglichkeiten, seine Konfiguration den individuellen Erfordernissen anzupassen. Die wichtigsten Optio-

nen und ihre Bedeutung werden im Folgenden erläutert. Für eine umfassende Beschreibung sei auf [Alm96] verwiesen.

Die Konfiguration von LILO wird in der Datei `/etc/lilo.conf` eingetragen. Bei einer Erstinstallation von Linux empfehlen wir, dies zunächst von YaST durchführen zu lassen. Eine eventuell nötige Nachbearbeitung von `lilo.conf` kann auf der von YaST erstellten Datei aufbauen.

Hinweis

Die Datei `/etc/lilo.conf` sollte nur für `root` lesbar sein, da sie Passwörter enthalten kann (vgl. Abschnitt 96); dies ist Standard bei SuSE Linux.

Hinweis

Es ist ratsam, die bei der letzten LILO-Installation verwendete Konfigurationsdatei sorgfältig aufzubewahren und vor jeder Änderung eine Sicherheitskopie herzustellen. Eine Änderung wird erst wirksam, indem Sie LILO mit der neuesten Fassung der Konfigurationsdatei neu installieren (Abschnitt *Installation und Deinstallation von LILO* auf Seite 100)!

Der Aufbau der Datei lilo.conf

Die `/etc/lilo.conf` beginnt mit einem *globalen Abschnitt* (engl. *global options section*) mit allgemeinen Einstellungen, gefolgt von einem oder mehreren *System-Abschnitten* (engl. *image sections*) für die einzelnen Betriebssysteme, die LILO starten soll. Ein neuer Systemabschnitt wird jeweils eingeleitet durch eine Zeile mit der Option `image` oder `other`.

Die Reihenfolge der einzelnen Betriebssysteme in der `lilo.conf` ist nur insofern von Bedeutung, als das *zuerst* in der Liste aufgeführte System automatisch gebootet wird, wenn keine Benutzereingabe erfolgt – gegebenenfalls nach Ablauf einer vorkonfigurierten Wartezeit (s. u. die Optionen `delay` und `timeout`).

Datei 2 zeigt eine Beispielkonfiguration auf einem Rechner mit Linux und Windows. Beim Booten sollen zur Auswahl stehen: ein neuer Kernel (`/boot/vmlinuz`) und ein Linux-Kernel als Fallback (`/boot/vmlinuz.shipped`, sowie Windows auf `/dev/hda1` und das Programm Memtest86.

```
### LILO global section
boot    = /dev/hda            # LILO installation target: MBR
backup  = /boot/MBR.hda.990428  # backup file for the old MBR
                                # 1999-04-28
vga     = normal              # normal text mode (80x25 chars)
```

```
read-only
menu-scheme = Wg:kw:Wg:Wg
lba32                        # Use BIOS to ignore
                             # 1024 cylinder limit
prompt
password = q99iwr4           # LILO password (example)
timeout = 80                 # Wait at prompt for 8 s before
                             # default is booted
message = /boot/message      # LILO's greeting

### LILO Linux section (default)
  image  = /boot/vmlinuz     # Default
  label  = linux
  root   = /dev/hda7         # Root partition for the kernel
  initrd = /boot/initrd

### LILO Linux section (fallback)
  image  = /boot/vmlinuz.shipped
  label  = Failsafe
  root   = /dev/hda7
  initrd = /boot/initrd.suse
  optional

### LILO other system section (Windows)
  other  = /dev/hda1         # Windows partition
  label  = windows

### LILO Memory Test
  image  = /boot/memtest.bin
  label  = memtest86
```

Datei 2: *Beispielkonfiguration in /etc/lilo.conf*

In `/etc/lilo.conf` ist alles von einem # bis zum Zeilenende Kommentar. Er wird – ebenso wie Zwischenraum – von LILO ignoriert und kann zur Verbesserung der Lesbarkeit verwendet werden. Zunächst werden die unbedingt notwendigen Einträge besprochen, die weiteren Optionen sind im anschließenden Abschnitt *Weitere optionale Konfigurationsmöglichkeiten* auf Seite 96 beschrieben.

- **Globaler Abschnitt** (Parameterteil)
  - ▷ `boot=`⟨*bootdevice*⟩

Device auf dessen erstem Sektor der LILO-Bootsektor installiert werden soll (das Installationsziel).
⟨*bootdevice*⟩ kann sein: ein Diskettenlaufwerk (`/dev/fd0`), eine Partition (z. B. `/dev/hdb3`), oder eine ganze Platte (z. B. `/dev/hda`): letzteres bedeutet die Installation im MBR.

Voreinstellung: Fehlt diese Angabe, wird LILO auf der gegenwärtigen Linux-Rootpartition installiert.

▷ `lba32`
Diese Option umgeht die 1024-Zylinder-Grenze von LILO. Dies funktioniert natürlich nur, wenn das BIOS Ihres Rechners dies auch unterstützt.

▷ `prompt`
Erzwingt das Erscheinen der LILO-Eingabeaufforderung (Prompt). Die Voreinstellung ist: kein Prompt! (Vgl. Abschnitt *Weitere optionale Konfigurationsmöglichkeiten* auf der nächsten Seite, Option `delay`.)

Empfohlen, sobald LILO mehr als nur ein System starten soll. Zusammen damit sollte auch die `timeout`-Option gesetzt werden, damit ein automatischer Reboot möglich ist, wenn keine Eingabe erfolgt.

▷ `timeout=`⟨*zehntelsekunden*⟩
Setzt eine Auszeit für die Wahl des zu startenden Systems und ermöglicht dadurch das automatische Booten, wenn nicht rechtzeitig eine Auswahl erfolgt. ⟨*zehntelsekunden*⟩ ist dabei die verbleibende Zeit in Zehntelsekunden für eine Eingabe. Durch Drücken von ⇑ wird diese Funktion außer Kraft gesetzt und der Rechner wartet auf Ihre Eingabe. Die Voreinstellung ist 80.

- **Linux-Abschnitt**

▷ `image=`⟨*kernelimage*⟩
Hier muss der Name des zu bootenden Kernel-Images stehen. Dies wird in der Regel `/boot/vmlinuz` sein.

▷ `label=`⟨*name*⟩
Innerhalb der `/etc/lilo.conf` eindeutiger, aber sonst frei wählbarer Name für das System (z. B. `Linux`). Maximale Länge 15 Zeichen: möglichst nur Buchstaben, Ziffern und Unterstrich – keine Leerzeichen, Sonderzeichen wie deutsche Umlaute u. Ä. Die genauen Regeln für erlaubte Zeichen finden Sie in [Alm96], Abschnitt 3.2.1. Voreinstellung: der Dateiname des Kernel-Images (z. B. `/boot/vmlinuz`).

Unter diesem Namen wählen Sie beim Systemstart das gewünschte Betriebssystem aus. Bei mehreren Systemen empfiehlt es sich, eine nähere Beschreibung der Namen und Systeme in einer message-Datei (siehe Abschnitt *Weitere optionale Konfigurationsmöglichkeiten* auf dieser Seite, Option `message`) bereitzustellen.

▷ `root=`⟨*rootdevice*⟩

Damit gibt LILO dem Kernel die Rootpartition (z. B. `/dev/hda2`) des Linux-Systems an. Zur Sicherheit empfohlen! Wird diese Option weggelassen, nimmt der Kernel die in ihm selbst eingetragene Rootpartition ⟨*kernelimage*⟩.

- **Linux-Abschnitt** (Linux – Safe Settings)

  Auch wenn ein eigener Kernel installiert wurde, ist es immer möglich, auf diesen Kernel zurückzugreifen und das System zu starten.

  ▷ `optional`

  Sollte `/boot/vmlinuz.shipped` gelöscht werden (*nicht* empfehlenswert!), wird bei der LILO-Installation dieser Abschnitt ohne Fehlermeldung übergangen.

- **Anderes System**

  ▷ `other=`⟨*partition*⟩

  Mit `other` werden LILO Startpartitionen anderer Systeme zum Booten bekannt gemacht (z. B. `/dev/hda1`).

  ▷ `label=`⟨*name*⟩

  Wählen Sie hier einen Name für dieses System. Die Voreinstellung – der bloße Device-Name der Partition – ist beim Booten nicht sehr aussagekräftig.

- **Memory Test**

  Hier ist nur das Programm zum Testen des Speichers eingetragen.

Weitere optionale Konfigurationsmöglichkeiten

Im letzten Abschnitt wurden nur die in `/etc/lilo.conf` minimal nötigen Einträge besprochen. Weitere nützliche Einstellungen folgen nun hier.

Jede Optionen wird als globale oder als Image-Optionen gekennzeichnet. Letztere gehören in den Abschnitt eines einzelnen Betriebssystems. Die anderen sind für den globalen Parameterteil von `/etc/lilo.conf` gedacht.

- `backup=`⟨*backup-Datei*⟩ (global)

  Die Datei, in der LILO ein Backup desjenigen Bootsektors ablegt, in den er anschließend installiert wird. Hierfür ist `/boot/boot.xxxx` die Vorgabe, wobei `xxxx` die interne Gerätenummer der Installationspartition ist; dies ist zu finden in den Kernelsourcen in `/usr/src/linux/init/main.c`, Funktion `parse_root_dev()`.

  Wir empfehlen, einen leichter deutbaren Namen zu verwenden, etwa wie oben im Beispiel (mit Gerätenamen und Datumsangabe). Sie verzichten damit auf das eingebaute Uninstall-Feature von LILO; aber dies macht man unser Meinung nach sowieso besser mit aller Sorgfalt von Hand (siehe auf Seite 102).

  Hinweis

  Wenn die Backup-Datei vorher schon vorhanden ist, legt LILO *kein* neues Backup an! Sorgen Sie daher dafür, dass hier jeweils ein neuer Dateiname verwendet wird.

  Hinweis

- `compact` (image)

  Diese Option empfiehlt sich bei Installation von LILO auf Diskette. LILO versucht dann, beim Start mehrere Sektoren auf einmal zu lesen und bootet unter Umständen schneller. Dies funktioniert leider nicht auf allen Maschinen. Bei der Installation von LILO sollten Sie darauf verzichten. Das ist sicherer und der Zeitgewinn beträgt nur wenige Sekunden.

- `loader=`⟨*Boot-Loader*⟩ (image)

  Für das Laden eines fremden Bootsektors baut LILO in seiner Map-Datei einen „Pseudo-MBR“ (beim Booten startet erst LILO den Pseudo-MBR, und dieser dann den fremden Bootsektor). Diese Option gibt die Datei an, aus der der Code für den Pseudo-MBR zu nehmen ist.

  Voreinstellung und generell richtig: `/boot/chain.b` .

  Manchmal soll ein Betriebssystem, das von der ersten Festplatte gebootet werden will (z. B. DOS), dennoch mit LILO von einer anderen Platte gestartet werden. Die Zusatzoptionen `map-drive=`⟨*Nummer*⟩ und `to=`⟨*Nummer*⟩ gestatten es, diese beiden Platten anhand ihrer BIOS-Gerätenummern zu „vertauschen“. Beispiel: Datei 3.

```
# Booting DOS from the second hard drive
# DOS bootable partition config begins
other = /dev/hdb1
```

```
  label = DOS
  loader = /boot/chain.b
     map-drive = 0x80    #  first hd: BIOS number 0x80
     to        = 0x81    # second hd: BIOS number 0x81
     map-drive = 0x81
     to        = 0x80
  table = /dev/hdb
# DOS bootable partition config ends
```

Datei 3: *Auszug aus /etc/lilo.conf: DOS von 2. Festplatte booten*

- `table=`⟨*ptabelle*⟩ (image)

  ⟨*ptabelle*⟩ muss das Quell-Device für die Partitionstabelle angeben, die in den Pseudo-MBR soll (in der Regel `/dev/hda` oder `/dev/sda`).

- `disk=`⟨*Gerätedatei*⟩ (global)
  `bios=`⟨*BIOS-Gerätenummer*⟩
  `cylinders=`⟨*Anzahl*⟩
  `heads=`⟨*Anzahl*⟩
  `sectors=`⟨*Anzahl*⟩

  Hier kann LILO für einzelne Festplatten direkt vorgeschrieben werden, welche BIOS-Gerätenummer und Geometrie er zur Adressierung von Sektoren dieser Platte verwenden soll. Dies ist nur sehr selten erforderlich! Die wichtigste Anwendung betrifft *IDE-SCSI-Mischsysteme*. Wenn Sie ein BIOS haben, das die Bootreihenfolge *SCSI vor IDE* erlaubt und Sie diese Möglichkeit nutzen wollen, muss LILO extra über die geänderte Reihenfolge der Festplatten aus BIOS-Sicht informiert werden. Dies geschieht durch Zusatzeintrag in den globalen Teil der `lilo.conf` wie z. B. in Datei 4 für den Fall eines Systems mit je einer IDE- und SCSI-Platte.

```
# Enable LILO to correctly access /dev/sda and /dev/hda
# at boot time if their boot order is interchanged in
# the BIOS:
disk = /dev/sda    #   The SCSI disk is regarded as ...
   bios = 0x80     #   ... first BIOS disk;
disk = /dev/hda    #   the IDE disk is regarded as ...
   bios = 0x81     #   ... second BIOS disk.
```

Datei 4: *Auszug aus lilo.conf: Bootreihenfolge: SCSI vor IDE*

- `linear` (global)

  Die Angabe dieser Option bewirkt, dass bei der Installation von LILO sämtliche Referenzen auf Plattensektoren als logische anstelle physikalischer Adressen abgelegt werden, sodass sie unabhängig von der Festplattengeometrie werden. Diese Option ist für den Fall gedacht, dass bei manchen Festplatten-Controllern das BIOS beim Systemstart eine andere Geometrie erkennt als das laufende Linux-System. Nur selten erforderlich!

  Die `linear` Option befreit *nicht* von der 1024-Zylinder-Grenze, die durch die BIOS-Geometrie der Boot-Festplatte festgelegt ist. Vgl. auch `file:/usr/share/doc/sdb/de/html/kgw_lilo_linear.html`.

- `message=`⟨*`message-datei`*⟩ (global)

  Verweist auf eine Datei, die den Bootbildschirm beim Systemstart erzeugt und die verschiedenen Betriebssysteme zur Auswahl anbietet. Nunmehr wird in der Regel ein PCX-Bild als Startmeldung eingesetzt; zur Hintergrund-Information vgl. `file:/usr/share/doc/sdb/de/html/jkoeke_bootgrafik.html`.

  Hinweis

  Wird diese Option verwendet, so gehört die `message`-Datei zur LILO-Startmaschinerie. Jede Änderung dieser Datei macht eine Neuinstallation von LILO erforderlich (Abschnitt *Installation und Deinstallation von LILO* auf der nächsten Seite)!

  Hinweis

- `password=`⟨*`passwort`*⟩ (global oder image)

  Kann sowohl am Anfang im globalen Parameter-Abschnitt, als auch in einzelnen Systemabschnitten stehen. Sichert den Zugriff auf die LILO--Dienste bzw. auf das Booten des betreffenden Systems mit einem Passwort ab.

  Hinweis

  Verwenden Sie bitte keine Sonderzeichen wie Umlaute und kein z oder y, da Sie noch eine amerikanische Tastatur haben, wenn LILO nach dem Passwort fragt. Um absolut sicher zu gehen, sollten Sie das nach der ersten Verwendung von `lilo.conf` gleich wieder herauslöschen – als `root` können Sie sowieso jederzeit durch Neu-Installation von LILO ein neues Passwort setzen.

  Hinweis

Es empfiehlt sich, zusätzlich die Option `restricted` zu setzen. Andernfalls kann man mit einem bestimmten Parameter direkt eine Shell starten; vgl. die Manual-Page von `lilo.conf` (`man lilo.conf`)!

- `read-only` (global)

  Mit dieser Image-Option weist LILO den betreffenden Kernel an, die Rootpartition zunächst read-only zu mounten, wie es beim Start von Linux- Systemen generell üblich ist. Wird diese Option weggelassen, verwendet der Kernel die in ihm selbst eingetragene Voreinstellung, die mit dem Kommando `rdev -R` ⟨*kernelimage*⟩ angezeigt wird.

- `delay=`⟨*zehntelsekunden*⟩ (global)

  Wenn der Prompt *nicht* zwingend vorgeschrieben worden ist, kann der Benutzer dennoch zur Startzeit von LILO durch Tastendruck (⇑, Ctrl, Alt) einen Prompt anfordern. Die `delay` Option gibt die Zeit vor, die LILO nach seinem Start auf einen solchen Tastendruck wartet, bevor er automatisch das erste System aus seiner Betriebssystem-Liste lädt. Die Voreinstellung ist `0`, d. h. keine Wartezeit.

  Die `delay` Option ist natürlich *überflüssig*, wenn mit `prompt` sowieso ein Prompt zwingend angefordert wird.

- `vga=`⟨*mode*⟩ (global)

  Wählt den VGA-Textmodus beim Start. Gültige Werte für ⟨*mode*⟩ sind `normal` (für 80x25), `ext` (für 80x50) oder `ask` (beim Booten fragen). Die bei Framebuffer-Kernel möglichen Werte sind in `/usr/src/linux/Documentation/fb/vesafb.txt` genannt und beschrieben.

- `append="`⟨*parameter*⟩`"` (image)

  Image-Option für Linux-Kernel. Ermöglicht die Übergabe von Kernel--Parametern wie etwa bei der Übergabe von Hardwarekomponenten, genauso wie dies am LILO-Prompt möglich ist. Der Kernel erhält zuerst die `append` Zeile, dann die Eingaben am Prompt; daher überwiegen im Zweifelsfall die Eingaben am Prompt.

  Zum Beispiel: `append="mcd=0x300,10"`

Installation und Deinstallation von LILO

Bei einer Neuinstallation von Linux führt YaST2 den Benutzer interaktiv durch die nötigen Schritte. Ein Eingreifen von Hand ist bei der Installation

von LILO im Allgemeinen nicht nötig. Hier möchten wir aber davon ausgehen, dass LILO mit speziellen Optionen in ein bestehendes System integriert werden soll.

Achtung

Die Installation eines Bootmanagers ist ein tiefer Eingriff ins System und dementsprechend heikel. Vergewissern Sie sich vor der Installation von LILO *auf jeden Fall*, dass Sie die anderen vorhandenen Betriebssysteme von Diskette booten können (funktioniert nicht bei Windows XP)! Vor allem fdisk muss zur Verfügung stehen. SuSE Linux kann gegebenenfalls auch von der Installations-CD bzw. -DVD gebootet werden.

Achtung

Installation nach Änderung der Konfiguration

Wenn sich an den LILO-Komponenten (siehe auf Seite 90) etwas geändert hat oder wenn Sie Ihre Konfiguration in `/etc/lilo.conf` modifiziert haben, müssen Sie LILO neu installieren. Dies geschieht durch einfachen Aufruf des sog. *Map-Installers*:

```
erde:~ #  /sbin/lilo
```

LILO legt daraufhin ein Backup des Ziel-(Boot-)Sektors an, schreibt seine „erste Stufe“ in diesen Sektor und erzeugt eine neue Map-Datei (siehe auf Seite 90). LILO meldet nacheinander die installierten Systeme – z. B. im Fall unser obigen Beispielkonfiguration:

```
Added linux *
Added suse
Added windows
Added memtest86
```

Nach abgeschlossener Installation kann der Rechner neu gestartet werden:

```
erde:~ #  shutdown -r now
```

Nachdem das BIOS seinen Systemtest ausgeführt hat, meldet sich LILO mit seiner Eingabeaufforderung, an der Sie LILO Parameter für den Kernel übergeben und das gewünschte Bootimage auswählen können. Mit (Tab) lassen sich die Bezeichnungen der installierten Konfigurationen auflisten.

Installation nach Neukompilierung des Kernels

Wenn Sie einen neu kompilierten Kernel in Ihr Bootkonzept aufnehmen wollen, haben Sie neben der LILO-Neuinstallation von Hand noch eine weitere, und zwar bequemere Möglichkeit:

Die Organisation der Befehle zum Konfigurieren und zum Erzeugen des Kernels ist in `/usr/src/linux/Makefile` niedergelegt; dort soll `INSTALL_PATH=/boot` festgelegt werden. Dieses `Makefile` verfügt über ein `target` namens `bzlilo`, das nach einer Kernel-Kompilierung automatisch den derzeit als `/boot/vmlinuz` (früher `/vmlinuz`) installierten Kernel nach `/boot/vmlinuz.old` kopiert, den neu erzeugten Kernel nach `/boot/vmlinuz` schreibt und schließlich LILO neu installiert. Dazu reicht:

```
erde:/usr/src/linux #  make bzlilo
```

Das ist freilich nur sinnvoll, wenn Ihre `/etc/lilo.conf` auf diesen LILO--Aufruf *vorher* vorbereitet worden ist und Ihr bisheriger Kernel wirklich unter `/boot/vmlinuz` liegt. Unter Ihren Images sollten Sie den neuen Kernel – und zur Sicherheit auch den alten – aufführen; etwa so, wie es in Datei 2 auf Seite 93 für `suse` geschehen ist. Wählen Sie beispielsweise als `label` den Namen `Linux.old`. Auf den `suse`-Kernel können Sie in jedem Fall zurückgreifen.

Dadurch können Sie am LILO-Bootprompt sowohl den neuen Kernel starten als auch den alten – funktionierenden – Kernel (Name im Beispiel: `Linux.old`). So bauen Sie eine weitere Sicherheitsstufe ein, die dann von Nutzen ist, wenn das System mit dem neuen Kernel nicht booten kann. Zum Erzeugen eines neuen Kernels siehe Kapitel 9 auf Seite 185 ff.

Entfernen von LILO

Achtung

Die Deinstallation eines Bootmanagers ist ein tiefer Eingriff ins System und dementsprechend heikel. Vergewissern Sie sich vor der Deinstallation von LILO *auf jeden Fall*, dass Sie Ihr Linux, und möglichst auch Ihre anderen Betriebssysteme – soweit vorhanden – von Diskette bzw. CD booten können! Sie geraten sonst möglicherweise in die unangenehme Lage, nicht mehr auf die Betriebssysteme auf Ihrer Festplatte zugreifen zu können.

Achtung

Um LILO zu deinstallieren, wird der Bootsektor, in dem LILO installiert worden ist, mit seinem früheren Inhalt überschrieben. Unter Linux ist das kein

Problem, *wenn* ein gültiges Backup vorhanden ist (vgl. Abschnitt *Weitere optionale Konfigurationsmöglichkeiten* auf Seite 96, Option `backup`). Auch YaST2 kann Sie in diesem Fall unterstützen.

Achtung

Ein Bootsektor-Backup wird ungültig, wenn die betreffende Partition ein neues Dateisystem erhalten hat. Die Partitionstabelle in einem MBR-Backup wird ungültig, wenn die betreffende Festplatte zwischenzeitlich anders partitioniert worden ist. Solche Backups sind „Zeitbomben“: am Besten sofort löschen!

Achtung

DOS oder Windows 95/98 MBR wiederherstellen

Am einfachsten ist es, einen DOS- oder Windows-MBR wiederherzustellen. Es geschieht mit dem MS-DOS-Befehl (verfügbar ab DOS-Version 5.0):

```
C:\> fdisk /MBR
```

bzw. dem OS/2-Befehl:

```
C:\> fdisk /newmbr
```

Diese Befehle schreiben nur die 446 ersten Bytes (den Boot-Code) in den MBR zurück und lassen die gegenwärtige Partitionstabelle unangetastet. Außer, wenn der MBR (siehe auf Seite 86) wegen einer falschen „magischen Zahl“ als im ganzen ungültig behandelt wird: dann wird die Partitionstabelle genullt! *Nicht vergessen:* Mit fdisk die von jetzt an gewünschte Startpartition wieder als *aktiv* (engl. *bootable*) kennzeichnen; die MBR-Routinen von DOS, Windows, OS/2 brauchen das!

Ansonsten legen Sie zunächst von dem fraglichen LILO-Sektor ein weiteres frisches Backup an – sicher ist sicher. Dann prüfen Sie, ob Ihre alte Backup--Datei die richtige ist und ob sie genau 512 Byte groß ist. Schließlich spielen Sie diese mit den folgenden Befehlen zurück:

- Wenn LILO in Partition yyyy (z. B. hda1, hda2,...) residiert:

  ```
  erde:~ #  dd if=/dev/yyyy of=Neue-Datei bs=512 count=1
  erde:~ #  dd if=Backup-Datei of=/dev/yyyy
  ```

- Wenn LILO im MBR der Platte zzz (z. B. hda, sda) residiert:

  ```
  erde:~ #  dd if=/dev/zzz of=Neue-Datei bs=512 count=1
  ```

```
erde:~ #  dd if=Backup-Datei of=/dev/zzz bs=446 count=1
```

Der letzte Befehl ist „vorsichtig" und schreibt gleichfalls nicht in die Partitionstabelle. Auch hier *nicht vergessen:* Mit fdisk anschließend die von jetzt an gewünschte Startpartition wieder als *aktiv* (engl. *bootable*) kennzeichnen.

Windows XP MBR wiederherstellen

Booten Sie von der Windows XP CD, drücken Sie im Setup die Taste Ⓡ, um die Wiederherstellungskonsole zu starten. Wählen Sie aus der Liste Ihre Windows XP Installation aus und geben Sie das Administratorpasswort ein. Geben Sie in die Eingabeaufforderung den Befehl `FIXMBR` ein und bestätigen Sie die Sicherheitsabfrage mit `j`. Mit `exit` können Sie den Computer anschließend neu starten.

Windows 2000 MBR wiederherstellen

Booten Sie von der Windows 2000 CD, drücken Sie im Setup die Taste Ⓡ, sowie im darauf folgenden Menü die Taste Ⓚ, um die Wiederherstellungskonsole zu starten. Wählen Sie aus der Liste Ihre Windows 2000 Installation aus und geben Sie das Administratorpasswort ein. Geben Sie in die Eingabeaufforderung den Befehl `FIXMBR` ein und bestätigen Sie die Sicherheitsabfrage mit `j`. Mit `exit` können Sie den Computer anschließend neu starten.

Beispielkonfigurationen

Wenn Ihr neues Linux allein auf dem System ist, besteht zunächst gar kein Handlungsbedarf, denn alles Nötige wurde im Rahmen der Installation unter YaST2 erledigt.

Weitere Informationen für Mehrsystem-Rechner finden Sie unter `/usr/share/doc/howto/en/html/mini/Linux+*`.

DOS/Windows 95/98 und Linux

Voraussetzung: Für DOS/Windows 95/98 und Linux steht jeweils eine primäre Partition unter der 1024-Zylinder-Grenze zur Verfügung (vgl. auf Seite 91); die Linux Boot-Partition kann auch eine logische Partition sein, sofern diese ganz unter der 1024-Zylinder-Grenze liegt.

Für diesen Fall wurde eine geeignete Konfiguration bereits besprochen (vgl. Datei 2 auf Seite 93) – nur die Angaben bei `root`, `image` und `other` sind an die tatsächlichen Verhältnisse anzupassen. LILO wird im MBR installiert.

Heben Sie die `/etc/lilo.conf` gut auf, außerdem sollten Sie die Installations-CD verfügbar haben, um das installierte Linux installieren zu können. Gerade Windows 95/98 neigt verschiedentlich dazu, „fremde“ MBRs kurzerhand zu eliminieren. Wenn Sie Linux danach noch mit einer Bootdiskette starten können, ist dieses Problem rasch behoben mit dem einfachen Befehl

```
erde:~ #  /sbin/lilo
```

Windows NT, 2000 oder XP und Linux

Grundsätzlich ist das Bootkonzept von Windows 2000, Windows NT und Windows XP identisch.

1. *Möglichkeit:* Zum Booten wird der *Bootmanager von Windows* benutzt. Dieser kann neben Bootsektoren auch Abbilddateien solcher Bootsektoren starten. Mit den folgenden Schritten lässt sich eine Koexistenz von Linux und Windows erreichen:

   (a) Installation von Windows 2000/NT/XP.

   (b) Einen Datenträger (Festplatten-Partition oder fehlerfreie Floppy) bereithalten mit einem Dateisystem, das Linux beschreiben und Windows lesen kann, z. B. FAT.

   (c) Linux wie „üblich“ installieren (als Root-Partition nehmen wir hier im Beispiel mal `/dev/sda3` an). FAT-Datenträger (z. B. unter `/dosa`) mounten. *Achtung: nicht* die verfälschenden `mount`-Optionen `conv=auto` oder `conv=text` verwenden!

   (d) LILO in der Linux-Rootpartition (also `/dev/sda3`) installieren, *nicht* in den MBR (`/dev/sda`)! Sie haben dabei nach wie vor die Möglichkeit, für LILO eine Auswahl unter mehreren Linux-Kernelimages zu konfigurieren. Beispiel:

```
# LILO Konfigurations-Datei: Rootpartition /dev/sda3
#                            startbar machen
# Start LILO global Section
boot=/dev/sda3                # Installationsziel
backup=/boot/boot.sda3.980428 # Backup für den vorigen
                              # Bootsektor
```

```
prompt
timeout=100     # Warten am Prompt: 10 s
vga = normal    # force sane state
# End LILO global section
# Linux bootable partition config begins
image = /boot/vmlinuz        #   default image to boot
    root = /dev/sda3         # Root-Partition hierher!
    label = Linux
# Linux bootable partition config ends
```

Nach der Änderung der `lilo.conf` den LILO wie gewohnt installieren:

```
erde:~ #  /sbin/lilo
```

(e) Kopieren des LILO-Bootsektors in eine Datei auf dem FAT-Datenträger, z. B.

```
erde:~ #  dd if=/dev/sda3 of=/dosa/bootsek.lin bs=512
    count=1
```

Dieser Schritt, wie auch der folgende, muss natürlich nach jedem Kernel-Update wiederholt werden!

(f) Windows booten. Die Datei `bootsek.lin` vom FAT-Datenträger ins Hauptverzeichnis des NT-Systemlaufwerks kopieren, falls die Datei nicht schon dort ist.

(g) In der Datei `boot.ini` (Attribute setzen) folgenden Eintrag am Ende ergänzen:
`c:\bootsek.lin="Linux"`

(h) Beim nächsten Booten sollte – wenn alles geklappt hat – ein entsprechender Eintrag im Windows-Bootmanager vorhanden sein!

2. *Möglichkeit, leider nicht immer praktikabel: LILO im MBR* installieren und für Windows so tun, als sei es DOS (wie im vorigen Beispiel); aber Achtung: Dies scheint bei neueren Versionen nicht mehr zu funktionieren, da es nur zu starten scheint, wenn es spezielle (undokumentierte) Sequenzen im MBR findet, von denen LILO leider nichts weiss.

Achtung

Windows NT/2000/XP kennen die von Linux verwendeten Partitionstypen 82 und 83 nicht! Achten Sie darauf, dass kein Windows-Programm die Partitionstabelle dahingehend „repariert“: es droht Datenverlust! Halten Sie sicherheitshalber gültige Backups des LILO-MBR bereit.

Achtung

Probleme mit LILO

Einige Richtlinien

Zu Beginn ein paar einfache Richtlinien, mit denen die meisten LILO--Probleme von vornherein vermieden werden können (entnommen dem LILO-Benutzerhandbuch [Alm96]):

- Halten Sie stets eine aktuelle und erprobte „Bootdiskette“ bereit.

  SuSE Linux enthält ein eigenständiges Rettungssystem (siehe Abschnitt 212), mit dem Sie an alle Linux-Partitionen wieder herankommen. Mit enthalten ist genügend Werkzeug, um die allermeisten Probleme mit unzugänglich gewordenen Festplatten zu lösen. Außerdem können Sie das installierte Linux auch von der Installations-CD booten.

- *Vor* jedem Aufruf des Map-Installers (`/sbin/lilo`), überprüfen Sie sorgfältig die Konfigurationsdatei `/etc/lilo.conf` .

- Rufen Sie `/sbin/lilo` *jedes Mal* auf, wenn irgendein Bestandteil der LILO-Startmaschinerie, die LILO-Konfigurationsdatei `/etc/lilo.conf`, der Kernel oder die initrd geändert worden sind.

Booten mit GRUB

Abgesehen von den bereits erwähnten Punkten, gelten die meisten Funktionen von LILO auch für GRUB. Einige Unterschiede werden dem Benutzer jedoch auffallen.

Wie LILO besteht GRUB auch aus zwei Stufen — eine erste 512-Byte-Stufe, die in den MBR oder einen Partitions-Boot-Block geschrieben wird, und eine größere zweite Stufe („stage2“), die durch eine Map-Datei gefunden wird. Ab diesem Punkt jedoch unterscheidet sich GRUB von LILO. stage2 kann auf Dateisysteme zugreifen. Derzeit werden ext2, ext3, reiser FS, jfs, xfs, minix und das von Windows verwendete DOS FAT FS unterstützt. Die Dateien eines solchen Dateisystems auf einem unterstützten BIOS-Disk-Device (Floppy oder vom BIOS erkannte Festplatten) können angezeigt, als Befehl oder Menüdatei verwendet oder als Kernel oder initrd in den Speicher geladen werden, lediglich durch Ausführung des entsprechenden Befehls, gefolgt vom BIOS-Device und einem Pfad.

Der größte Unterschied zu LILO besteht darin, dass, wenn GRUB einmal installiert ist, Kernel- und Menüeinträge ohne weiteres Zutun hinzugefügt oder

geändert werden können. GRUB wird beim Booten dynamisch die Inhalte der Dateien finden und erneut einlesen.

Das Menü

Nach erfolgter Installation ist die Menüdatei die wichtigste GRUB-Datei für den Anwender. Diese befindet sich standardmäßig unter `/boot/grub/menu.lst`. Sie enthält alle Informationen zu anderen Partitionen oder Betriebssystemen, die mithilfe des Menüs gebootet werden können.

GRUB liest bei jedem Systemstart die Menüdatei vom Dateisystem neu ein. Es besteht also kein Bedarf, GRUB nach jeder erfolgten Änderung an der Datei zu aktualisieren — verwenden Sie einfach YaST2 oder Ihren favorisierten Editor.

Die Menüdatei enthält Befehle. Die Syntax ist sehr einfach. Jede Zeile enthält einen Befehl, gefolgt von optionalen Parametern, die wie bei der Shell durch Leerzeichen getrennt werden. Einige Befehle erlauben aus historischen Gründen ein Gleichheitszeichen vor dem ersten Parameter. Kommentare werden durch einen Hash ('#') eingeleitet.

Zur Erkennung der Menüeinträge in der Menüübersicht, müssen Sie für jeden Eintrag einen Namen oder einen `title` vergeben. Der nach dem Schlüsselwort `title` stehende Text wird inklusive Leerzeichen im Menüs als selektierbare Option angezeigt. Alle Befehle bis zum nächsten `title` werden nach Auswahl dieses Menüeintrages ausgeführt.

Einfachster Fall ist das Verzweigen zu Bootloadern anderer Betriebssysteme. Der Befehl lautet `chainloader` und das Argument ist normalerweise der Boot Block einer anderen Partition in GRUBs *Block-Notation*, zum Beispiel:

```
chainloader (hd0,3)+1
```

Die Gerätenamen unter GRUB werden in Abschnitt *Namen für BIOS-Geräte* auf der nächsten Seite erklärt. Obiges Beispiel spezifiziert den ersten Block der vierten Partition auf der ersten Festplatte.

Mit dem Kommando `kernel` wird ein Kernel-Image spezifiziert. Das erste Argument ist der Pfad zum Kernel-Image auf einer Partition. Die restlichen Argumente werden dem Kernel auf der Kommandozeile übergeben.

Wenn der Kernel nicht die erforderlichen Treiber für den Zugriff auf die root-Partition einkompiliert hat, dann muss `initrd` angegeben werden. Hierbei handelt es sich um einen separaten GRUB-Befehl, der den Pfad zur initrd-Datei als einziges Argument hat. Da die Ladeadresse der initrd in das bereits

geladene Kernel-Image geschrieben wird, muss der Befehl `initrd` auf den `kernel`-Befehl folgen.

Der Befehl `root` vereinfacht die Spezifikation der Kernel- und initrd-Dateien. Genaugenommen macht dieser Befehl gar nichts; er vereinfacht die Eingabe von Pfaden in das Dateisystem. `root` hat als einziges Argument entweder ein GRUB-Device oder eine Partition auf einem solchen. Allen Kernel-, initrd-, oder anderen Dateipfaden, bei denen nicht explizit ein Device angegeben wird, wird bis zum nächsten `root`-Befehl das Device vorangestellt.

Am Ende jeden Menüeintrags steht implizit das `boot`-Kommando, so dass dieses nicht in die Menüdatei geschrieben werden muss. Sollten Sie jedoch in die Situation kommen, GRUB interaktiv zum Booten zu benutzen, müssen Sie am Ende das `boot`-Kommando eingeben. `boot` hat keine Argumente, es führt lediglich das geladene Kernel-Image oder den angegebenen Chain Loader aus.

Wenn Sie alle Menüeinträge geschrieben haben, müssen Sie einen Eintrag als `default` festlegen. Andernfalls wird der erste (Eintrag `0`) verwendet. Sie haben auch die Möglichkeit, einen Timeout in Sekunden anzugeben, nach dem dies geschehen soll. `timeout` und `default` werden üblicherweise vor die Menüeinträge geschrieben.

Namen für BIOS-Geräte

Die Herkunft von GRUB zeigt sich in der Weise, wie es Namen an BIOS-Devices vergibt. Es wird ein BSD-ähnliches Schema verwendet: die Diskettenlaufwerke `0x00, 0x01` werden fd0 und fd1 genannt und alle Festplatten (`0x80, 0x81, 0x82`), die vom BIOS oder durch Zusatz-Controller erkannt werden, werden als hd0, hd1 etc. bezeichnet, unabhängig vom Typ des Controllers. Das Problem, dass Linux-Device-Namen nicht eindeutig zu BIOS-Device-Namen zugeordnet werden können, besteht für sowohl LILO als auch GRUB. Beide benutzen vergleichbare Algorithmen, um diese Zuordnung zu generieren. Jedoch speichert GRUB diese Zuordnung in einer Datei, die bearbeitet werden kann.

Festplattenpartitionen werden durch Anhängen eines Kommas und der Partitionsnummer spezifiziert. Ein kompletter GRUB-Pfad besteht aus einem Device-Namen, der in Klammern geschrieben wird sowie dem Pfad der Datei in dem Dateisystem auf der angegebenen Partition. Der Pfad wird durch einen Slash eingeleitet. Als Beispiel, auf einem System mit einer einzelnen IDE-Festplatte und Linux auf der ersten Partition, könnte der bootbare Kernel

wie folgt aussehen

```
(hd0,0)/boot/vmlinuz
```

Hinweis

Die Zählung der Partitionen in GRUB beginnt bei Null. (hd0,0) entspricht /dev/hda1.

Hinweis

Installation mit der GRUB-Shell

GRUB existiert in zwei Versionen. Einmal als Booloader und einmal als normales Linux-Programm. Dieses Programm wird als *GRUB shell* bezeichnet. Beide haben die Möglichkeit, GRUB als Bootloader auf eine Festplatte oder Diskette zu installieren, entweder mit dem Kommando `install` oder `setup`. Dadurch vereinfacht sich die Rettung eines defekten Systems.

Nur wenn es als Linux-Programm läuft, kommt der Zuordnungsalgorithmus ins Spiel. Das Programm liest die Datei `device.map`, welche aus Zeilen besteht, die jeweils GRUB-Device und Linux-Device-Namen enthalten. Da die Reihenfolge von IDE, SCSI und anderen Festplatten abhängig von verschiedenen Faktoren ist, und Linux die Zuordnung nicht erkennen kann, besteht die Möglichkeit, die Reihenfolge in der `device.map` festzulegen. Sollten Sie Probleme beim Booten haben, kontrollieren Sie, ob die Reihenfolge in dieser Datei der BIOS-Reihenfolge entspricht. Die Datei befindet sich im GRUB-Verzeichnis `/boot/grub/`.

Einrichten des Bootmechanismus mit loadlin

Es soll nun mit loadlin noch eine weitere Methode vorgestellt werden, SuSE Linux zu booten. loadlin ist ein DOS-Programm, das in der Lage ist, einen in einem DOS-Verzeichnis gespeicherten Linux-Kernel zu starten. loadlin fügt sich nahtlos in eine bestehende DOS/Windows 9x-Umgebung ein und kann mit Hilfe des Windows Bootmanagers komfortabel gestartet werden. Da kein Eintrag in den MBR erfolgt, sieht Windows von Linux lediglich eine oder mehrere Partitionen mit ihm unbekannten Kennungen (engl. *IDs*). Die Gefahr unerwünschter Nebeneffekte aufgrund der Existenz von Linux auf Ihrem System ist so minimiert.

Das hier beschriebene Vorgehen funktioniert auf Windows 95 und Windows 98. Die gezeigten Konfigurationsdateien wurden unter Windows 95 entwickelt; es ist deshalb im Folgenden nur von Windows 95 die Rede.

Wenn Sie loadlin verwenden möchten, um Ihr Linux zu starten, müssen Sie diesen Weg vorbereiten. Je nach Systemgegebenheiten müssen Sie auch einige Startdateien modifizieren.

Prinzipiell können Sie loadlin auf zwei Arten aktivieren: indem Sie beim Systemstart via Bootmenü zwischen mehreren Konfigurationen wählen oder indem Sie aus dem laufenden System heraus loadlin aktivieren und zu Linux überwechseln.

Beide Methoden haben Ihre Vor- und Nachteile:

- Das Bootmenü spart den Umweg über ein anderes Betriebssystem, um Linux zu starten.
- In ein Bootmenü können Sie weitere Konfigurationen einbauen und sich so einen universellen Startmechanismus aufbauen.
- Sie müssen allerdings die Startdateien modifizieren, um ein Bootmenü aufzubauen; eventuell ist dazu Probieren nötig. In den DOS-Hilfedateien können Sie eventuell fündig werden; geben Sie einmal `help menu` ein.
- Am DOS-Prompt ist der Wechsel zu Linux sehr einfach.
- Unter Windows 95 kann man den Linux-Start schön in die grafische Oberfläche integrieren. Mit einem Doppelklick auf ein Icon können Sie zu Linux wechseln. Es ist jedoch auch unter Windows 95 ein Bootmenü möglich (Windows 95 enthält DOS 7.0).

Tipp

Verwenden Sie nach Möglichkeit ein Boot-Menü, wenn Sie nach dem Einschalten direkt Linux booten wollen. Die DOS-Prompt- bzw. Doppelklick-Methode kann zusätzlich verwendet werden, wenn Sie von DOS/Windows 95 nach Linux wechseln wollen.

Mit Startmenüs und der Windows 95-Konfiguration kann man sich recht intensiv auseinandersetzen – Sie werden verstehen, dass wir das Thema hier nur recht gradlinig behandeln.

Tipp

Notwendige Dateien für loadlin

Das müssen Sie immer tun (unter DOS, Windows 3.x und Windows 95):

1. Vermutlich haben Sie loadlin bereits installiert. Wenn nicht, müssen Sie zuerst loadlin von der CD installieren (z. B. mit YaST2).

2. Wechseln Sie (unter MS-DOS) in das Verzeichnis `c:\loadlin`. Dort finden Sie eine Datei `linux.par`. Erstellen Sie mit einem Editor in diesem Verzeichnis eine Datei mit Namen `startlin.bat` (oder einem anderen, Ihnen passenden Namen). In die Datei schreiben Sie diese Zeile:

   ```
   c:\loadlin\loadlin @c:\loadlin\linux.par
   ```

   Nun editieren Sie in der Datei `linux.par` die folgenden Zeilen:

   ```
   c:\loadlin\zimage    # first value must be
                        # the filename of the Linux-kernel
   initrd=c:\loadlin\initrd
   root=/dev/xxx        # the device which gets mounted as root FS
   ro                   # mount root read-only
   ```

   Statt `xxx` tragen Sie den Devicenamen Ihrer Rootpartition ein. Den `initrd`-Eintrag benötigen Sie nur, wenn Sie beispielsweise SCSI-Unterstützung gleich beim Booten hinzuladen müssen (zum Konzept der „initial ramdisk“ vgl. Abschnitt *Problemstellung* auf Seite 202).
   Mit der Datei `startlin.bat` können Sie Ihr Linux jederzeit vom DOS-Prompt aus starten. Die Datei `linux.par` wird sowohl von `startlin.bat` als auch von `config.sys` verwendet und enthält alle zum Booten von Linux notwendigen Parameter. Wenn Sie mit Linux vertraut geworden sind, können Sie in `linux.par` auch andere Boot--Parameter einfügen und/oder ersetzen. Haben Sie sich später einmal Ihren eigenen Kernel gebaut, kopieren Sie diesen vom Linux-Filesystem nach `c:\loadlin\zimage` und es wird fortan dieser Kernel gebootet; bei Bedarf müssen Sie dort auch eine neu generierte `initrd` ablegen.

Bootmenüs einrichten

So richten Sie ein Bootmenü unter DOS bzw. Windows 3.x ein:

1. Als erstes müssen Sie in der Datei `c:\config.sys` ein Bootmenü definieren. Tragen Sie dazu etwas ähnliches wie in Datei 5 ein.

```
[Menu]
menuitem=Win, Windows starten...
menuitem=DOS, MS-DOS starten...
menuitem=Linux, Linux starten...
menucolor=15,1
menudefault=Win,5
```

***Datei 5:** Beispiel für config.sys (1. Teil) für den Linux-Start*

Unter dem Label `[Menu]` definieren Sie die Einträge des Bootmenüs, seine Farbe und nach wie viel Sekunden welcher Menüpunkt automatisch aufgerufen werden soll.

2. Weiter unten tragen Sie die Labels [Common], [Win], [DOS] und [Linux] ein. Bei Common schreiben Sie die Einträge hin, die immer gelten sollen; bei den anderen Labels notieren Sie die Einträge, welche nur bei einem bestimmten Eintrag gelten. Verwenden Sie dazu die Zeilen, die in Ihrer jetzigen `config.sys` stehen:

```
[Common]
device=c:\dos\himem.sys /testmem:off
device=c:\dos\emm386.exe noems
dos=high,umb
files=30
buffers=10
shell=c:\dos\command.com

[Win]
devicehigh=c:\dos\dblspace.sys /move
devicehigh=c:\cd\slcd.sys /D:SONY_000 /B:340 /M:P /V /C

[DOS]
devicehigh=c:\dos\dblspace.sys /move
devicehigh=c:\cd\slcd.sys /D:SONY_000 /B:340 /M:P /V /C

[Linux]
shell=c:\loadlin\loadlin.exe @c:\loadlin\linux.par

[Common]
rem Bleibt leer
```

Speichern Sie die Datei dann ab.

3. Öffnen Sie jetzt die Datei `c:\autoexec.bat`. In die Datei müssen Sie die gleichen Labels schreiben und den Labels Einträge zuordnen, die

Notation ist jetzt aber etwas anders. Welches Label im Bootmenü gewählt wurde, steht in der Variablen `%config%`. Hier ein Beispiel:

```
@echo off

rem Einträge für alle Konfigurationen
switches= /f
set comspec=c:\dos\command.com
prompt $p$g
loadhigh c:\dos\keyb gr,,c:\dos\keyboard.sys
loadhigh c:\dos\doskey
set temp=c:\temp
loadhigh c:\dos\mscdex.exe /D:SONY_000 /E /V /L:H
c:\logimaus\mouse.exe

goto %config%

:Win
c:\dos\smartdrv.exe a- b- c+ 2048 1024
path c:\windows;c:\dos;c:\util;
win
c:\dos\smartdrv /C
goto ende

:DOS
path c:\dos;c:\util;
goto ende

:ende
echo * Auf Wiedersehen *
```

4. Wenn Sie den Rechner jetzt booten, erscheint das Bootmenü und Sie haben 5 Sekunden Zeit, einen Eintrag auszuwählen. Nach 5 Sekunden startet automatisch Windows. Wenn Sie 'Linux' auswählen, startet Linux und wartet auf Ihr Login.

Von Windows aus starten

So richten Sie ein Start-Icon für Linux ein, mit dem Sie Linux aus einem laufenden Windows 95-System booten können:

1. Klicken Sie sich in den Ordner `c:\loadlin` hinein, markieren Sie die Datei `startlin.bat` und wählen Sie im Bearbeiten-Menü 'Kopieren' aus.

2. Gehen Sie in einen Ordner oder auf den Desktop, je nachdem, wo Sie Ihr Linux-Icon haben möchten. Drücken Sie die rechte Maustaste und wählen Sie 'Verknüpfung einfügen'.

3. Markieren Sie die gerade eingefügte Verknüpfung, drücken Sie die rechte Maustaste und wählen Sie 'Eigenschaften'. Gehen Sie in das Register 'Programm', klicken Sie unten auf den Knopf 'Erweitert'. Kreuzen Sie in der Maske das Feld 'MS-DOS-Modus' an. Bestätigen Sie mit 'OK'.

4. Über den Knopf 'Anderes Symbol' können Sie sich ein schönes Icon aussuchen und geben Sie der Verknüpfung einen passenden Namen. Fertig!

5. Ein Doppelklick auf das neue Symbol bringt eine Bestätigungsmaske, dass sich Windows 95 jetzt in den MS-DOS-Modus bemüht. Falls Sie die Maske nervt: Ausschalten in den Eigenschaften der Verknüpfung.

Das Windows Startmenü

So richten Sie ein Startmenü für Windows 95 ein:

1. Zuerst müssen Sie die Datei `c:\msdos.sys` editieren. Dazu machen Sie die Datei mittels

   `C:> **attrib -R -S -H c:\msdos.sys**`

   sichtbar. Es ist eine Textdatei, in die Sie einige Zeilen einfügen müssen, um das Windows 95-eigene Startmenü zu aktivieren. Unter dem Label `[Options]` sollte es etwa so aussehen wie in Datei 6.

```
[Options]
BootGUI=0
BootDelay=0
BootMenu=0
Logo=0
```

Datei 6: *msdos.sys für den Linux-Start*

Der Parameter `Logo=0` ist optional und verhindert, dass Windows 95 vor dem Booten in den Grafikmodus schaltet; das Booten geht dann schneller und Sie haben weniger Ärger, wenn sie später unter Linux den DOS-Emulator verwenden wollen.

Der Parameter `BootGUI=0` bewirkt, dass Windows 95 direkt in den DOS-Modus bootet. Nach dem Editieren der Datei setzen Sie die Attribute wieder zurück. Um Windows dann zu starten muss

```
C:> win
```

am DOS-Prompt eingegeben werden, aber das tut schon unsere Beispieldatei `c:\autoexec.bat`, wenn Sie im Menü Win95 gewählt haben.

2. Dann müssen Sie in der Datei `c:\config.sys` Ihr eigenes Bootmenü definieren. Tragen Sie dazu am Anfang der Datei etwa den Inhalt ein:

```
[Menu]
menuitem=Win95, Windows 95 starten...
menuitem=DOS, MS-DOS starten...
menuitem=Linux, Linux starten...
menudefault=Win95,5
```

Unter dem Label `[Menu]` definieren Sie die Einträge des Bootmenüs und nach wie viel Sekunden welcher Menüpunkt automatisch aufgerufen werden soll.

3. Weiter unten stehen Labels `[Win95]`, `[DOS]`, `[Linux]` und `[Common]`. Bei `[Common]` schreiben Sie die Einträge hin, die immer gelten sollen (unter Windows 95 werden das nur wenige sein); bei den anderen Labels die Einträge notieren, welche nur bei einem bestimmten Eintrag des Bootmenüs gelten. Verwenden Sie dazu die Zeilen, die in Ihrer jetzigen `config.sys` stehen; ein Beispiel als Anregung:

```
[Win95]
dos=high,umb
device=c:\windows\himem.sys /testmem:off

[DOS]
device=c:\plugplay\drivers\dos\dwcfgmg.sys
dos=high,umb
device=c:\windows\himem.sys /testmem:off
device=c:\windows\emm386.exe noems I=B000-B7FF
devicehigh=c:\cdrom\torisan.sys /D:TSYCD3 /P:SM

[Linux]
shell=c:\loadlin\loadlin.exe @c:\loadlin\linux.par

[Common]
accdate=C+ D+ H+
switches= /F buffers=20
```

Speichern Sie die Datei dann ab.

4. Öffnen Sie jetzt die Datei `c:\autoexec.bat`. In die Datei müssen Sie die gleichen Labels schreiben und den Labels Einträge zuordnen, die Notation ist jetzt aber etwas anders. Welches Label im Bootmenü gewählt wurde, steht in der Variablen %config%. Schreiben Sie etwa folgendes:

```
@echo off
loadhigh keyb gr,,c:\windows\command\keyboard.sys
goto %config%

:Win95
win
goto ende

:DOS
path c:.;d:.;c:\windows\command;c:\util;
loadhigh c:\windows\command\mscdex.exe /D:TSYCD3 /L:x
loadhigh c:\windows\command\doskey
c:\windows\command\mouse.exe
goto ende

:ende
echo * Und jetzt? *
```

5. Wenn Sie den Rechner jetzt booten, erscheint Ihr eigenes Bootmenü. Sie haben 5 Sekunden Zeit zum Wählen, dann startet automatisch Windows 95. Wenn Sie 'Linux' auswählen, startet Linux und wartet auf Ihr Login.

Für alle Fälle: Boot-CD erstellen

Falls Sie Probleme haben, Ihr installiertes System über einen Bootmanager zu booten oder Lilo oder Grub nicht in den MBR Ihrer Festplatte installieren wollen, ist es auch möglich, eine bootfähige CD zu erstellen, auf die Sie die Linux Startdateien brennen. Vorraussetzung hierfür ist natürlich, daß ein Brenner in Ihrem System vorhanden und eingerichtet ist.

Boot-CD mit ISOLINUX

Um eine bootfähige CD zu erstellen, ist es am einfachsten, den Bootmanager Isolinux zu verwenden. Auch die SuSE Installations-CDs werden übrigens per Verwendung von Isolinux bootfähig gemacht.

- Booten Sie Ihr installiertes System zunächst auf folgendem Umweg (ab SuSE Linux 7.2):

  ▷ Booten Sie von der Installations-CD oder -DVD, wie bei der Installation.

  ▷ Wählen Sie beim Booten die Option 'Installation' aus (ist voreingestellt).

  ▷ Danach Sprache und Tastaturbelegung auswählen.

  ▷ Im nächsten Menu wählen Sie den Punkt 'Installiertes System booten'.

  ▷ Die root-Partition wird automatisch erkannt und von dieser wird das System gebootet.

- Installieren Sie mit Hilfe von YaST2 das Paket `syslinux`.

- Öffnen Sie eine Root-Shell. Mit Hilfe der folgenden Aufrufe wird für die Boot-CD ein temporäres Verzeichnis erstellt und die zum Booten des Linux Systems notwendigen Dateien (der Bootloader Isolinux sowie der Kernel und die Initrd) hineinkopiert.

  ```
  erde:~ #  mkdir /tmp/CDroot
  erde:~ #  cp /usr/share/syslinux/isolinux.bin /tmp/CDroot/
  erde:~ #  cp /boot/vmlinuz /tmp/CDroot/linux
  erde:~ #  cp /boot/initrd /tmp/CDroot
  ```

- Mit Ihrem Lieblingseditor erstellen Sie nun die Bootloader-Konfigurationsdatei `/tmp/CDroot/isolinux.cfg`. Wenn Sie z. B. `pico` verwenden wollen, lautet der entsprechende Aufruf

  ```
  pico /tmp/CDroot/isolinux.cfg
  ```

  Tragen Sie folgenden Inhalt ein:

  ```
  DEFAULT linux
  LABEL linux
    KERNEL linux
    APPEND initrd=initrd root=/dev/hdXY [bootparameter]
  ```

  Für den Parameter `root=/dev/hdXY` tragen Sie bitte Ihre root-Partition ein. Wenn Sie sich nicht sicher sind, welche Partitionsbezeichnung diese hat, schauen Sie einfach in der Datei `/etc/fstab` nach. Für den Wert

[bootparameter] können Sie zusätzliche Optionen eingeben, die beim Booten verwendet werden sollen. Die Konfigurationsdatei könnte z. B. folgendermaßen aussehen:

```
DEFAULT linux LABEL linux KERNEL linux APPEND initrd=initrd
root=/dev/hda7 hdd=ide-scsi
```

- Anschließend wird mit folgendem Aufruf aus den Dateien ein ISO9660-Dateisystem für die CD erstellt (schreiben Sie das folgende Kommando in eine Zeile):

```
mkisofs -o /tmp/bootcd.iso -b isolinux.bin -c boot.cat
  -no-emul-boot -boot-load-size 4
  -boot-info-table /tmp/CDroot
```

- Dann kann die Datei /tmp/bootcd.iso auf CD gebrannt werden, entweder mit graphischen Brennprogrammen wie KonCD oder XCDroast, oder einfach von der Kommandozeile:

```
cdrecord -v speed=2 dev=0,0,0 /tmp/bootcd.iso -eject
```

  Evtl. muss der Parameter dev=0,0,0 an die SCSI-ID des Brenners angepasst werden (diese erfahren Sie durch Eingabe des Aufrufs cdrecord -scanbus, vgl. auch Manual-Page von cdrecord (man cdrecord)).

- Probieren Sie die Boot-CD aus! Rebooten Sie dazu den Computer und überprüfen Sie ob Ihr Linux-System korrekt von der CD gestartet wird.

Sound mit ALSA

ALSA – http://www.alsa-project.org. Die Grundlagen aus dem Handbuch [SuS02c] sind für das Verständnis der folgenden Abschnitte hilfreich.

Die grundlegenden PCM-Typen 122
Audiodaten komprimieren 122
Buffering und Latenzen 123
ALSA und Midi 125
MIDI ohne WaveTable-Karte abspielen 131
arecord und aplay 134
Linux für DJs – GDAM und terminatorX 134

Grundlegende PCM-Typen: hw und plughw

Durch die Auswahl eines bestimmten PCM-Typs kann der Anwender beeinflussen, wie ALSA auf die Soundkarte zugreift. Die wichtigsten PCM-Typen tragen die Namen `hw` und `plughw`.

Um den Unterschied zu beleuchten, muss kurz auf die Vorgänge beim Öffnen eines PCM-Device eingegangen werden. Dieses muss mit bestimmten Einstellungen für (mindestens) folgende Parameter geöffnet werden: Sample-Format, Sample-Frequenz, Anzahl der Kanäle, Anzahl der Perioden (früher „Fragments“ genannt) und Größe einer Periode. Nun kann es passieren, dass eine Applikation z. B. eine WAV-Datei mit einer Sample-Frequenz von 44,1 kHz abspielen möchte, die Soundkarte aber diese Frequenz nicht unterstützt. In diesem Fall kann ALSA im Plugin-Layer eine automatische Konvertierung der Daten in ein Format vornehmen, welches von der Soundkarte unterstützt wird. Die Konvertierung betrifft die Parameter Sample-Format, Sample-Frequenz und Anzahl der Kanäle.

Die Zuschaltung des Plugin-Layers wird durch die Auswahl des PCM-Typs `plughw` aktiviert. Mit dem PCM-Typ `hw` versucht ALSA dagegen direkt, die PCM-Devices mit den von der Applikation benötigten Parametern zu öffnen.

Die Angabe der gewünschten Soundkarten- und Device-Nummer folgt nach einem Doppelpunkt auf den PCM-Typ. Dabei wird zuerst die Karten- und dann die Device-Nummer angegeben. Der komplette Bezeichner für ein PCM-Device sieht also z. B. so aus:

```
erde:~ #  plughw:0,0
```

Audiodaten komprimieren

Paket `cdparanoia`
Paket `vorbis-tools`

Unter `http://www.xiph.org/paranoia/doc.html` finden Sie eine Beschreibung zu `cdparanoia`. Zur Erinnerung, mit einem Kommando wie

```
erde:~ #  cdparanoia -B -z "1-3"
```

werden die Tracks 1 bis 3 als WAV-Dateien gespeichert, wobei cdparanoia selbstständig nach einem Laufwerk mit eingelegter Audio-CD sucht.

Unter KDE können Audio-CDs sogar per „Drag & Drop“ gerippt werden. Wenn Sie Konqueror starten und `audiocd:/` als ‘URL’ eingeben, werden

die Tracks einer eingelegten Audio-CD sowie mehrere virtuelle Verzeichnisse angezeigt. Mehr darüber können Sie im Abschnitt „Audio CDs grabben mit dem Konqueror" lesen, den Sie im Handbuch [SuS02c] im Kapitel „CDs brennen mit KOnCD" finden.

Unkomprimierte Audiodaten in CD-Qualität belegen pro Minute fast 10 MB. Um diese Datenmengen drastisch zu komprimieren wurde am Fraunhofer IIS das MP3-Verfahren entwickelt. Leider ist dieses Verfahren patentiert. Firmen, die MP3-Encoder vertreiben, müssen daher Lizenzgebühren zahlen. Unter Linux wurde zwar der sehr leistungsfähige MP3-Encoder Lame entwickelt. Leider dürfen wir jedoch diesen Encoder nicht in unsere Distribution aufnehmen, obwohl der Quellcode von Lame unter GPL steht. Über die rechtliche Lage können Sie sich z. B. auf der Webseite des Projekts unter `http://lame.sourceforge.net` informieren. Die Benutzung von Lame ist in einigen Ländern, darunter Deutschland und den USA, ausschließlich zu Forschungszwecken gestattet.

Ein freies komprimierendes Audioformat ist Ogg Vorbis. Das Ogg-Format wird bereits von KOnCD, xmms, terminatorX und vielen anderen Playern unterstützt. Die Webseite des Projekts ist `http://www.xiph.org/ogg/vorbis`. Im Paket vorbis-tools sind u. A. ein Encoder und einfacher Player enthalten. Der Encoder wird von der Kommandozeile mit `oggenc` gestartet. Als einziger Parameter muss die zu komprimierende WAV-Datei übergeben werden. Mit der Option `-h` erhalten Sie eine Übersicht über weitere Parameter. In der neuesten Version unterstützt der Ogg-Encoder sogar die Kodierung mit variabler Bitrate. Auf diese Weise kann bei gleichbleibender Qualität eine noch höhere Komprimierung erreicht werden. Man kann nun statt der Bitrate den Parameter `-q` für die gewünschte Qualität angeben. Alternativ kann man aber auch weiterhin Parameter für die Bitrate angeben. Mit dem Parameter `-b` wird die durchschnittliche Bitrate festgelegt. Mit `-m` und `-M` kann die minimale und maximale Bitrate spezifiziert werden.

Ein Ogg-Player für die Kommandozeile ist ogg123. Dem Programm muss ein Device für die Wiedergabe übergeben werden. Sie starten das Programm mit einem Befehl wie

```
erde:~ #  ogg123 -d alsa09 mysong.ogg
```

Buffering und Latenzen

In diesem Abschnitt geht es um die Frage, wie man eine unterbrechungsfreie Audio-Wiedergabe sicherstellen kann. Die Problematik ist keineswegs Linux-spezifisch, sondern besteht bei sämtlichen Multitasking-Betriebssystemen. Bei

einem Multitasking-Betriebssystem laufen normalerweise mehrere Prozesse gleichzeitig. Da der Prozessor stets nur einen Prozess bearbeiten kann, wird den Prozessen durch den so genannten Scheduler des Betriebssystems Prozessor-Zeit zugeteilt. Dieses Umschalten zwischen den Prozessen geschieht normalerweise so schnell, dass der Anwender davon nichts merkt.

Bei der Audio-Wiedergabe würden sich aber bereits kurze Unterbrechungen durch Klicks bemerkbar machen. Audio-Programme verwenden daher einen Puffer (Buffering) für die Wiedergabe. Die Audio-Daten, die sich im Puffer befinden, werden auch dann weiter von der Soundkarte ausgegeben, wenn das Audio-Programm vom Scheduler unterbrochen wurde. Die Wiedergabe ist also dann klickfrei, wenn der Puffer groß genug ist, um auch die größtmögliche Unterbrechung zu überbrücken.

Die Puffergröße bestimmt die Reaktionszeit (Latenz) des Programms. Besonders bei interaktiven Anwendungen, wie Echtzeit-Synthesizern und DJ-Mixer-Konsolen versucht man daher, die Puffergröße möglichst klein zu halten. Grundsätzlich hängt die Dauer der Unterbrechungen von der Systemauslastung und der Priorität des Prozesses ab. Daraus folgt, dass sich die Größe des für klickfreie Wiedergabe benötigten Puffers verringern lässt, indem die Priorität des Audio-Programms erhöht wird. Viele Audio-Programme versuchen daher, ihren Prozess auf Echtzeit-Priorität umzustellen. Dies ist jedoch nur dann möglich, wenn sie mit `root`-Privilegien laufen.

Es ist immer ein Risiko, ein Programm im `root`-Modus laufen zu lassen, da dem Programm in diesem Fall alles erlaubt ist. Ein nicht vertretbares Sicherheitsrisiko ergibt sich, wenn der Rechner mit dem Internet verbunden ist. In diesem Fall können Sicherheitslücken des Programms ausgenutzt werden, um sich Zugang zum System zu verschaffen.

Achtung

Die im folgenden beschriebenen Befehle sollten also *niemals* auf Rechnern ausgeführt werden, auf die vom Internet aus zugegriffen werden kann, oder bei denen ein Systemabsturz oder Datenverlust schwerwiegende Folgen hätte.

Achtung

Um ein Programm im `root`-Modus auszuführen, sollte man den `sudo`-Mechanismus verwenden. Dieser soll am Beispiel des Programms timidity++ erläutert werden. Um allen Benutzern auf ihrem System die Ausführung von timidity++ mit `root`–Privilegien zu ermöglichen, müssen Sie die Datei `/etc/sudoers` anpassen; zum Vorgehen vgl. Manual-Page von `sudo` (`man sudo`) und Manual-Page von `sudoers` (`man sudoers`). Rufen Sie als `root` `visudo` auf und fügen Sie die folgende Zeile am Ende der Datei `/etc/sudoers` ein:

```
ALL     ALL=(ALL) /usr/bin/timidity
```

Es ist nun jedem Benutzer des Systems erlaubt, mit

```
erde:~ #  sudo timidity
```

das timidity im `root`-Modus zu starten. Dabei wird die Eingabe eines Passworts verlangt (dies ist das Passwort des jeweiligen Benutzers), falls seit dem letzten `sudo`-Kommando mehr als fünf Minuten vergangen sind.

ALSA und Midi

Paket `alsa, pmidi, aseqview, vkeybd`
Paket `awesfx, snd_sf2, kalsatools`

Neben der Möglichkeit, PCM-Daten wiederzugeben, verfügen viele Soundkarten auch über Midi-Funktionalität. Der ALSA Midi-Sequenzer implementiert eine kraftvolle Architektur für das Routing von Midi-Daten.

Viele Soundkarten besitzen einen externen Midi-Port zum Anschluss von Midi-Geräten wie Synthesizern, Keyboards und Klangmodulen. Wird der Midi-Port der Karte von ALSA unterstützt, können Sie über diesen Port mit einem Sequenzer-Programm (z. B. jazz) Midi-Dateien aufnehmen und wiedergeben. Einen Überblick über die von Ihrer Karte zur Verfügung gestellten Midi-Devices erhalten Sie im KDE-Kontrollzentrum unter dem Menüpunkt 'Klänge' → 'Midi'. Hier können Sie auch einstellen, welches dieser Devices zur Wiedergabe von Midi-Dateien verwendet werden soll. Auf der Kommandozeile können Sie sich die zur Verfügung stehenden Midi-Devices sowie deren internen ALSA Port-Nummern mit dem Kommando

```
erde:~ #  pmidi -l
```

auflisten lassen. Bei einer „Soundblaster Live!“-Karte sieht dieses Listing z. B. so aus:

```
Port     Client name                       Port name
 72:0     External MIDI 0                   MIDI 0-0
 73:0     Emu10k1 WaveTable                 Emu10k1 Port 0
 73:1     Emu10k1 WaveTable                 Emu10k1 Port 1
 73:2     Emu10k1 WaveTable                 Emu10k1 Port 2
 73:3     Emu10k1 WaveTable                 Emu10k1 Port 3
```

Datei 7: Midi-Devices einer Soundblaster Live!

In der ersten Spalte stehen die interne Port-Nummer, unter der das Device vom ALSA-Treiber angesprochen wird. In den übrigen Spalten stehen Bezeichnung und Portname des Device. Neben dem bereits erwähnten externen Midi-Port tauchen hier mehrere WaveTable-Ports auf. Mit einem Kommando wie z. B.

```
erde:~ #  pmidi -p 73:0 mysong.mid
```

können Sie eine Midi-Datei über einen der aufgelisteten Ports spielen lassen.

Hinweis

Wird ein Midi-Spieler während der Wiedergabe abgebrochen, so bleibt möglicherweise ein dauerhafter Klang zurück. Rufen Sie in diesem Fall das Skript `all_notes_off` auf. Wenn das nicht funktioniert, können Sie ALSA mit `rcalsasound restart` als `root` neu starten.

Hinweis

Viele Soundkarten (z. B. Soundblaster AWE und Live!) besitzen einen internen WaveTable-Synthesizer. Dieser wandelt Midi-Ereignisse in hörbare Klänge um.

Diese Midi-Ereignisse können entweder von einem externen Midi-Keyboard oder von einem Programm (z. B. Midi-Player oder Sequenzer) an den WaveTable-Synthesizer geschickt werden. Bei Soundblaster-AWE- und -Live!-Karten muss der WaveTable Synthesizer mit einem so genannten Soundfont initialisiert werden, bevor Klänge hörbar werden. Für Besitzer einer solchen Karte wird diese Initialisierung im nächsten Abschnitt beschrieben.

Soundfonts laden (SB Live! und AWE)

Das Paket `awesfx` enthält das Kommando `sfxload` zum Laden von Soundfonts in Soundblaster AWE und Live! Karten. Geeignete Soundfont-Dateien befinden sich z. B. auf der Treiber-CD Ihrer Soundkarte. Das Startup-Script von ALSA kann die für die WaveTable-Synthese benötigten Soundfonts automatisch laden. Voraussetzung dafür ist, dass mit YaST2 entsprechende Dateien von der Creative Driver CD installiert wurden. Das Script funktioniert momentan nur für eine Soundkarte. ALSA kann aber problemlos bis zu 8 Soundkarten verwalten. Das Laden der Soundfonts kann dann mit einem Kommando wie

```
erde:~ #  sfxload -D ⟨n⟩ /usr/share/sfbank/creative/8MBGMSFX.SF2
```

vorgenommen werden. ⟨*n*⟩ steht dabei für die Nummer der Soundkarte (0, 1...). Zu beachten ist, dass ⟨*n*⟩ nicht notwendigerweise die Nummer ist, unter der die Soundkarte konfiguriert wurde, sondern von der Reihenfolge abhängt, mit der die einzelnen Soundtreiber geladen wurden. Falls Sie Ihre Treiber-CD gerade nicht zur Hand haben, können Sie auch einen der unter `/usr/share/sounds/sf2` installierten Soundfonts laden.

Der Soundfont `Vintage_Dreams_Waves_v2.sf2` von Ian Wilson enthält 128 analoge Synthesizer-Klänge sowie 8 Drumsets. Er ist sowohl für SB-AWE-, als auch für -SB Live!-Karten geeignet.

Der ROM-Soundfont `gu11-rom.sf2` von Samuel Collins ist *nur* für SB AWE Karten geeignet. Er stellt für diese Karten eine erweiterte General Midi Bank zur Verfügung. Bitte beachten Sie die Copyright-Dateien und die Dokumentation unter `/usr/share/doc/packages/snd_sf2`.

Weitere Soundfonts finden Sie im Internet z. B. unter `http://www.hammersound.net`

vkeybd – virtuelles Midi-Keyboard

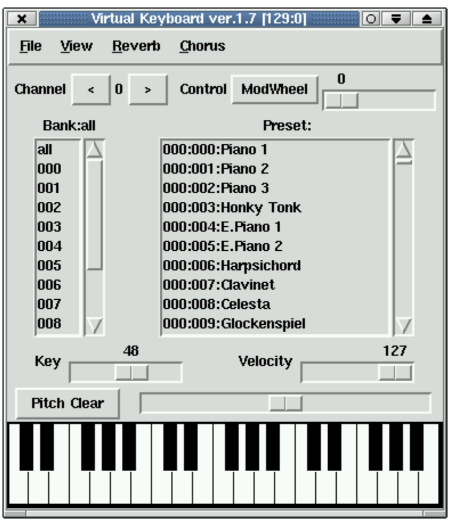


Abbildung 6.1: *vkeybd – vollständige virtuelle Midi-Tastatur*

Falls Sie kein externes Midi-Keyboard an Ihre Soundkarte angeschlossen haben, können Sie das virtuelle Keyboard vkeybd verwenden. Hier werden die internen Port-Nummern wichtig, die wir oben bereits mit `pmidi -l` aufgelistet haben. Das Programm wird von der Kommandozeile aufgerufen mit

```
erde:~ #  vkeybd --addr 73:0 &
```

Die Portadresse kann natürlich auf Ihrem System anders sein. Geben Sie hier den ersten WaveTable-Port aus der Liste an. Wenn Sie einen externen Tongenerator angeschlossen haben, können Sie natürlich auch die Port-Nummer des externen Midi-Ports angeben. vkeybd kennt noch eine Reihe weiterer Optionen. Mit

```
erde:~ #  vkeybd --addr 73:0 --octave 5 &
```

können Sie z. B. die Zahl der dargestellten Oktaven auf 5 erweitern.
Eine Übersicht über die Kommandozeilenoptionen erhalten Sie mit `vkeybd --help` bzw. in der Manual-Page von `vkeybd` (`man vkeybd`).

Die in der Preset-Liste dargestellten Instrumentbezeichnungen können durch Angabe einer Preset-Datei mit der Option `--preset` konfiguriert werden.
Die Instrumentnamen einer Soundfont-Datei können mit dem Kommando `sftovkb` extrahiert werden:

```
erde:~ #  cd /usr/share/sounds/sf2
erde:/usr/share/sounds/sf2 #  sftovkb Vintage_Dreams_Waves_v2.sf2
     \
     >~/vintage.vkb
```

speichert die Namen im Home-Verzeichnis in `vintage.vkb`. Die Oberfläche von vkeybd lässt sich über das Menü 'view' konfigurieren.

Verbindungen zwischen Midi Ports herstellen

ALSA stellt eine leistungsfähige Infrastruktur zum Verbinden verschiedener Midi-Ports zur Verfügung. Soundkarten und Midi-Programme (sofern diese die ALSA-Sequenzer-Struktur unterstützen) besitzen einen oder mehrere Midi-Ports, über die sie miteinander kommunizieren können. Die Verbindung der Ports kann entweder mit dem KDE-Programm kaconnect oder dem Kommando `aconnect` vorgenommen werden. Nach dem Programmstart zeigt kaconnect die auf dem System verfügbaren lesbaren und schreibbaren MIDI-Ports sowie deren Verbindungsstatus an. Zu Demonstrationszwecken können Sie einmal mit

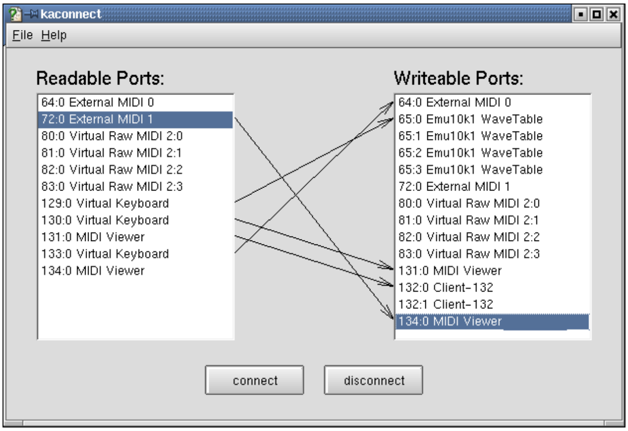


Abbildung 6.2: *Mit kaconnect Midi-Ports verbinden und Status anzeigen*

```
erde:~ #  vkeybd
erde:~ #  aseqview
```

zwei Midi-Programme starten. In der ist nach dem Programmnamen die Portadresse des Programms angegeben. Das erste Programm erhält z. B. die Portnummer `128:0`, das zweite `129:0`. Die Ports der Programme werden auch unmittelbar von kaconnect angezeigt.

Da vkeybd ohne den Parameter `--addr` aufgerufen wurde, kann jetzt die Verbindung zwischen dem Programm-Port und dem WaveTable-Port (oder dem externen Midi-Port) sozusagen per Hand hergestellt werden. Selektieren Sie dazu die entsprechenden Ports und klicken Sie dann auf 'connect'.

Falls Sie das Kommandozeilentool `aconnect` verwenden möchten, geben Sie

```
erde:~ #  aconnect 128:0 73:0
```

ein (oder etwas Entsprechendes). Damit wird eine (unidirektionale) Verbindung zwischen dem Port `128:0` als Sender und `73:0` als Empfänger hergestellt.

Sie können nun noch eine Verbindung zwischen dem Midi-Port des Keyboards und dem Midi-Port des ALSA Sequenzer Viewers herstellen. Falls Sie dann am Keyboard z. B. das Panning ändern oder das Pitchwheel (muss erst unter 'View' aktiviert werden) betätigen, so wird dies sofort von aseqview angezeigt.

Mit `aconnect -il` bzw. `aconnect -ol` können Sie die zum Empfang bzw. Senden zur Verfügung stehenden Ports und ihren Verbindungsstatus auflisten. Die mit `aconnect` hergestellten Verbindungen können Sie mit der `-d` Option wieder lösen, also z. B. mit

```
erde:~ #  aconnect -d 128:0 129:0
```

Wollen Sie sämtliche Verbindungen lösen, geht dies mit `aconnect -x`. Eine Übersicht über weitere Kommandozeilenoptionen von `aconnect` können Sie in der Manual-Page von `aconnect` (`man aconnect`) nachlesen.

Tipp

Für Experten: Mit `aseqnet` lassen sich Midi-Verbindungen über die Grenzen des eigenen Rechners hinaus auch im Netzwerk herstellen. Vielleicht wollen Sie ja mal mit einem alten Freund in Amerika vierhändig Klavier spielen...

Tipp

kmid – Der KDE Midi-Spieler

Paket `kdemultimedia`

Im KDE-Startmenü finden Sie unter 'Multimedia' den Menüpunkt 'Midi/Karaoke-Spieler'. Einige Demodateien für kmid liegen im Verzeichnis `/opt/kde2/share/apps/kmid` im `.kar`-Format vor. In diesen Dateien ist auch der Liedtext gespeichert, der synchron zur Wiedergabe gescrollt und markiert wird.

Midi-Dateien finden Sie im Internet an unzähligen Stellen. Eine nahe liegende Adresse ist z. B. `http://www.midi.net`. Ein umfangreiches Midi-Archiv klassischer Musik finden Sie unter `http://www.classicalarchives.com`

Die ausführliche Online-Hilfe von kmid kann mit F1 aufgerufen werden. Auch bei diesem Programm müssen wieder die Midi-Ports im Menü 'Einstellungen' unter 'Midi-Einstellungen' korrekt gewählt werden.

Bemerkenswert ist die Kanalansicht, die Sie erhalten, wenn Sie auf den Tastatur-Button in der Werkzeugleiste klicken; eventuell müssen Sie das Fenster etwas nach rechts aufziehen, damit dieser Punkt sichtbar wird. In der Kanalansicht – auch dieses Fenster muss eventuell in der Größe angepasst werden – werden die Midi-Ereignisse grafisch auf mehreren Tastaturen gezeigt. Außerdem können hier die Instrumente geändert werden.

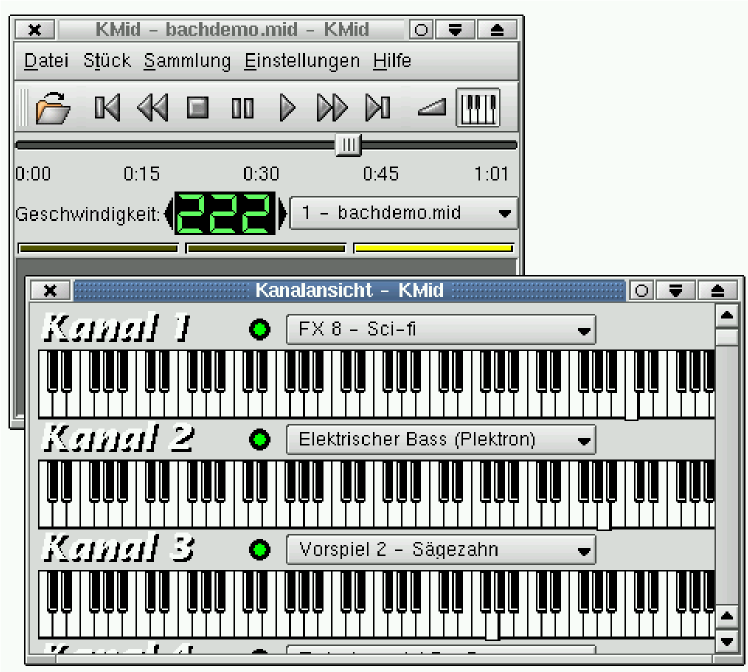


Abbildung 6.3: Hauptfenster und Kanalansicht von kmid

Eine mögliche Falle bei diesem Programm: Wird kmid durch Klick auf eine Midi-Datei im KDE-Dateimanager Konqueror aufgerufen, gelten die im KDE-Kontrollzentrum eingestellten Midi-Einstellungen. Wird das Programm separat aufgerufen, gelten die im Programm selbst vorgenommenen Einstellungen.

MIDI ohne WaveTable-Karte abspielen

Paket `timidity`

Nicht jede Soundkarte besitzt einen WaveTable-Synthesizer, mit dem MIDI-Dateien dem geladenen Soundfont (oder Instrumenten-Patch) entsprechend wiedergegeben werden können. In diesem Fall hilft der Software-WaveTable-Synthesizer timidity++ weiter.

Konfiguration von timidity++

timidity++ wird über die Konfigurationsdatei `/usr/share/timidity/timidity.cfg` konfiguriert. Es gibt eine eigene Dokumentation für die Konfiguration. Sie wird mit `man timidity.cfg` aufgerufen. Bitte lesen Sie auch die Dokumentation in `/usr/share/doc/packages/timidity`

Geeignete Instrumenten-Patches finden Sie unter `http://www.stardate.bc.ca/eawpatches/html/default.htm`

Von dort können Sie die Datei `eawpats11_full.rar` laden. Sie ist 22 MB groß, es lohnt sich aber, denn Sie erhalten damit ein vollständiges GM/GS/XG Instrumenten-Set. Damit Sie die Patches mit timidity nutzen können, müssen Sie wie folgt vorgehen: Werden Sie `root`. Legen sie ein Verzeichnis `/usr/share/timidity/eawpats` an, kopieren Sie `eawpats11_full.rar` dorthin und wechseln Sie in das Verzeichnis. Dies Kommando entpackt das Archiv:

```
erde:~ #  unrar x eawpats11_full.rar
```

Im Verzeichnis `/usr/share/timidity/` muss nun noch die Datei `timidity.cfg` angepasst werden. Diese soll nur noch aus den zwei Zeilen bestehen:

```
dir /usr/share/timidity/eawpats
source timidity.cfg
```

Datei 8: *timidity.cfg*

Achtung: Auch `eawpats11_full.rar` enthält eine Datei `timidity.cfg`, die sich nach dem Entpacken im Verzeichnis eawpats befindet. Diese wird durch das `source`-Kommando eingefügt. In dieser Datei sind nur diese vier Zeilen wichtig:

```
source gravis.cfg
source gsdrums.cfg
source gssfx.cfg
source xgmap2.cfg
```

Alle anderen Zeilen können gelöscht werden. Es müssen nun noch die Dateirechte aktualisiert werden. Geben Sie dazu den Befehl `chmod -R a+r /usr/share/timidity/eawpats` ein.

Falls Sie Soundfonts statt der Gravis Instrument Patches verwenden möchten, müssen Sie die Datei `/usr/share/timidity/timidity.cfg` ändern. Um

z. B. den Vintage Dreams Soundfont mit timidity++ zu benutzen, genügt ein `timidity.cfg`, bestehend aus nur einer einzigen Zeile:

```
soundfont /usr/share/sounds/sf2/Vintage_Dreams_Waves_v2.sf2
```

Mehr zu diesem Thema ist in `/usr/share/doc/packages/timidity/C/README.sf` zu finden.

timidity++ mit grafischer Oberfläche starten

Es gibt wohl nur wenige Programme, die dem Anwender eine so große Zahl möglicher Programmoberflächen anbieten, wie timidity++. Eine Übersicht erhalten Sie mit `man timidity`. Eine ausgereifte Oberfläche ist das „Athena Widget Interface". Dieses Interface wird gestartet mit

```
erde:~ #  /usr/bin/timidity -iatv &
```

Hinweis

Wenn Sie timidity starten, dürfen Sie sich *nicht* im Verzeichnis `/usr/share/timidity` befinden.

Hinweis

Eine eindrucksvolle Midi-Datei zur Demonstration des vollen Orchesterklangs ist z. B. die Aufnahme des ersten Satzes aus der 1. Sinfonie von Brahms, die Sie unter `http://www.classicalarchives.com/brahms.html` herunterladen können.

Der ALSA-Server Modus von timidity++

Sie starten timdity++ im ALSA Server-Modus mit

```
erde:~ #  /usr/bin/timidity -iA -B2,8 -Os &
```

Es wird dann u. A. eine Meldung wie

```
Opening sequencer port: 128:0 128:1
```

ausgegeben, in der der MIDI-Port angezeigt wird, über den der Synthesizer angesprochen werden kann (z. B. mit `vkeybd --addr 128:0`).

Falls Sie timidity++ wieder beenden wollen, können Sie mit

```
erde:~ #  killall timidity
```

alle timidity-Prozesse abbrechen.

WAV-Dateien aufnehmen und wiedergeben

Paket `alsa`

`arecord` und `aplay` sind deswegen interessant, weil sie direkt zum ALSA-Paket gehören und eine einfache und flexible Schnittstelle zu den PCM-Devices bieten.

Mit `arecord` und `aplay` können Audiodaten u. a. im Format WAV aufgenommen und wiedergegeben werden. Das Kommando

```
erde:~ #  arecord -t 10 -m mysong.wav
```

nimmt eine WAV-Datei von 10 Sekunden Länge auf. Die vollständige Liste der Optionen von `arecord` und `aplay` wird aufgelistet, wenn die Programme mit der `-h` Option aufgerufen werden. Achten Sie bitte bei der Aufnahme auf korrekte Einstellung des Mixers. Bei alsamixer betrifft dies die Regler 'Capture', und, je nach Aufnahmequelle, die Regler 'Line' oder 'MIC'. Außerdem muss die Aufnahmequelle korrekt gewählt sein.

Die Signalquelle wird bei der Aufnahme von einem Analog/Digital-Wandler digitalisiert. Bei einem 16 Bit-Wandler entspricht die maximale Amplitude der Zahl 65535. Ein höheres Signal wird stark verzerrt, da es ebenfalls in eine Schwingung mit Amplitude 65535 umgewandelt wird.

Linux für DJs – GDAM und terminatorX

Paket `gdam`, `terminatorX`, `gdam`

Auch für den DJ gibt es unter Linux einige kraftvolle Programme. Zwei besonders interessante Programme sollen in diesem Abschnitt vorgestellt werden. Beide Programme erlauben das Abmischen mehrerer MP3-Dateien und verfügen über eine Vielzahl von Effekten.

GDAM – Die Komplettlösung für den DJ

GDAM ist eine DJ-Mixer-Applikation, die kaum einen Wunsch offen lässt. Die Highlights:

- Client-Server Architektur ermöglicht gleichzeitige Wiedergabe beliebig (nur durch die Hardware begrenzt) vieler MP3-Dateien, auch via Netzwerk.

- Gleichzeitige Wiedergabe auf mehreren Soundkarten möglich (z. B. für zusätzliche Kopfhörer)
- Dynamisches Einfügen unzähliger Effekt-Plugins, darunter Spatial Stereo, Flanger, Respeed (bei konstantem Pitch).
- Unterstützung von zwei Tastaturen und Midi zur Bedienung der Steuerkonsole

Das Programmpaket enthält eine mehr als achtzigseitige Dokumentation, die Sie im Verzeichnis `/usr/share/doc/packages/gdam` finden. Lesen Sie dazu bitte auch die Datei `README_SuSE` im gleichen Verzeichnis. Der folgende Abschnitt gibt eine kurze Einführung.

Konfiguration des GDAM-Servers

Bevor Sie GDAM starten können, müssen Sie in Ihrem Home-Verzeichnis die Konfigurationsdatei für den GDAM-Server erstellen. Das ist nicht schwierig, denn Sie können dazu einfach die Beispielkonfiguration aus dem Verzeichnis `/usr/share/doc/packages/gdam` übernehmen. Legen Sie zunächst das Verzeichnis `~/.gdam` an, falls dieses nicht bereits existiert. Kopieren Sie dann die Datei `server.config_SuSE` nach `~/.gdam/server.config`. Die einzigen Zeilen, die ggf. geändert werden müssen, sehen so aus:

```
Device "oss" "/dev/dsp" "numfragments=3:logfragsize=12"
#Device "oss" "/dev/dsp1" "numfragments=3:logfragsize=12"
```

Der Server ist also für die Ausgabe mit OSS und einer Soundkarte konfiguriert. Wenn Sie mehr als eine Soundkarte verwenden möchten, müssen Sie das Kommentarzeichen in der zweiten Zeile löschen. Wichtig sind ferner die Parameter für das Buffering. `numfragments` bestimmt die Anzahl der Puffer und `logfragsize` deren Größe (die tatsächliche Größe in Bytes berechnet sich daraus gemäß $\text{Puffer} = 2^{\text{logfragsize}}$).

Weitere Hinweise zur Konfiguration finden Sie in der Datei `/usr/share/doc/packages/gdam/README.SuSE`.

Programmstart und Song Database Builder

Starten Sie den GDAM-Server von der Kommandozeile mit

```
gdam-server --config ~/.gdam/server.config &
```

Durch diesen Befehl wird der Server im Hintergrund gestartet. Sie können ihn mit `killall gdam-server` beenden. Wenn Sie GDAM mit Echtzeit-Priorität laufen lassen wollen, um niedrige Latenz zu erreichen, genügt

es, nur den Server im `root`-Modus laufen zu lassen. Wenn Sie den `sudo`-Mechanismus verwenden, sollte der Server nicht mit im Hintergrund gestartet werden, da Sie ihn dann nur als `root` wieder beenden können. Starten Sie den Server ohne &, können Sie ihn mit Ctrl + C beenden.

Achtung

Es muss an dieser Stelle darauf hingewiesen werden, dass es immer ein Sicherheitsrisiko ist, ein Programm als `root` zu starten. Mehr zu diesem Thema finden Sie im Abschnitt *Buffering und Latenzen*.

Achtung

Wenn der Server läuft, können Sie mit dem GDAM-Launcher Clients starten. Sie starten ihn mit

```
gdam-launcher --device /dev/dsp
```

Falls Sie mehr als eine Soundkarte konfiguriert haben, können Sie zusätzlich einen zweiten `-device` Parameter übergeben.

Es öffnen sich das 'launcher'-Fenster sowie ein Fenster 'song database warning'. Klicken Sie in letzterem auf die Buttons 'launch song selector' und 'launch database builder'. Mit dem 'Song Database Builder' können Sie nach MP3-Dateien suchen lassen und diese in die 'Song Database' aufnehmen. Geben Sie das gewünschte Verzeichnis für die

Suche an und klicken Sie dann auf 'Run Find'. Alternativ dazu können Sie unter 'Arbitrary command' auch eine Eingabe wie z. B. `ls ~/soundfiles/*.mp3` vornehmen und auf 'Run Arbitrary Command' klicken. Die gefundenen MP3-Dateien werden im 'GDAM Song Selector' aufgelistet. Sie können die Liste dort mit 'Save' abspeichern. Falls Sie mit der Option `-database` keine andere Datei angeben, sucht GDAM bei einem erneuten Programmstart nach der Liste in der Datei `~/.gdam/song.database`. Es ist daher sinnvoll, diesen Dateinamen zu verwenden. Klicken Sie zum Abspeichern auf den 'Save'-Button links neben dem Eingabefeld.

An den zahlreichen Meldungen, die von GDAM zur Laufzeit ausgegeben werden, erkennen Sie, dass sich das Programm noch in Entwicklung befindet. Lassen Sie sich von diesen Meldungen nicht irritieren.

Musik abspielen mit dem Wheels-Player

Starten Sie nun im 'Launcher'-Fenster den 'Wheels'-Player durch Mausklick auf das Symbol rechts neben dem Button 'wheels'. Es wird dann ein Doppel-Turntable geöffnet. Markieren Sie nun einige Songs im 'Song Selector'. Die selektierten Songs werden durch Mausklick auf das gelbe Pfeilsymbol (links

in der Anzeige der 'Wheels') in den Turntable geladen. Der 'Song Selector' kann übrigens jederzeit durch Mausklick auf das gelbe 'O'-Symbol (ebenfalls links in der Anzeige der 'Wheels') geöffnet und geschlossen werden.

Hinweis

Wenn Sie MP3-Dateien von einem CD-ROM-Laufwerk abspielen, beachten Sie bitte, dass möglichst nur ein Turntable auf das Laufwerk zugreifen sollte. Es kann sonst zu Problemen mit dem Buffering kommen.

Hinweis

Die Abspielliste des jeweiligen Turntables können Sie sich durch Mausklick auf das unscheinbare gelbe Symbol ˆ (rechts neben dem 'S'-Symbol) anzeigen lassen. Wenn Sie im Fenster 'Queued Songs' einen Song markieren und dann auf 'Skip' klicken, wird dieser Song in den Turntable geladen. Über den Button 'Source' oder das bereits erwähnte gelbe 'S'-Symbol können Sie einen Filebrowser aufrufen, mit dem sich weitere Songs zur Abspielliste hinzufügen lassen.

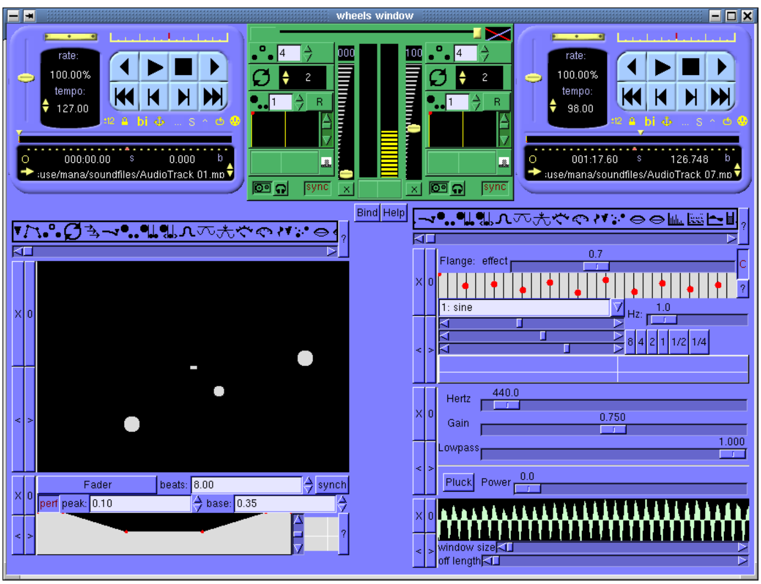


__Abbildung 6.4:__ Die „Wheels" von GDAM mit einigen Plugins

Im 'Wheels'-Fenster befindet sich am oberen Rand des grünen Bereichs ein Crossfader. Unmittelbar links davon finden Sie ein kleines Feld mit Koordina-

tensystem (im folgenden kurz xy-Feld genannt). Sie können damit die Form der Überblendkurven verändern. Letztere werden rechts neben dem Crossfader dargestellt. Wenn Sie diesen Crossfader zu langweilig finden, können Sie auch den Equalizer-Crossfader verwenden, der sich in Form eines xy-Felds unterhalb der Pegelanzeigen befindet.

Rechts neben den Equalizer-Feldern der Turntables befindet sich je ein kleiner Schalter für den ‘equalize mode’. Um einen Crossfade-Effekt zu erhalten, müssen Sie für die zwei Turntables entgegengesetzte Equalizer-Modi verwenden.

Im unteren Teil des ‘Wheels’-Fensters befinden sich die Plugin-Leisten. Hier finden Sie u. A. einzählige LADSPA-Plugins. Sie können die Effekt-Plugins einfach per Mausklick dynamisch einfügen. Jeder geöffnete Plugin verfügt über vier Buttons. Mit ‘0’ können Sie das Plugin temporär deaktivieren. Mit ‘X’ wird der Plugin entfernt. Mit ‘<’ bzw. ‘>’ können Sie die Reihenfolge der Plugins verändern. Nach dem Entfernen von Plugins wird der untere Fensterrand nicht automatisch nach oben verschoben. Falls sich der Fensterrand bereits aus dem Bildschirmbereich herausbewegt hat, können Sie ihn wie folgt wieder „einfangen“: Klicken Sie links in der Fensterleiste auf das graue Symbol ‘-’. Klicken Sie dann auf Größe und bewegen Sie den Mauszeiger nach unten. Klicken Sie dann noch einmal um den „Resize“-Modus zu verlassen.

Und nun viel Spaß beim Experimentieren mit den unzähligen Effekten. Versäumen Sie nicht, das ‘Respeed’-Plugin auszuprobieren. Sie können damit die Abspielgeschwindigkeit bei gleich bleibender (!) Tonhöhe verändern. Im Zusammenhang mit diesem Plugin treten Ringing-Artefakte auf. Diese können verringert werden, indem das „window“ von 1024 auf 4096 vergrößert wird.

Der Beat Calculator

Viele Effekte lassen sich an den Rhythmus des Songs anpassen. Einige Effekte funktionieren nur dann, wenn das ‘Tempo’-Feld des Songs nicht Null anzeigt. Sie können das Tempo im ‘beat calculator’ bestimmen. Klicken Sie dazu auf den entsprechenden Button im GDAM-launcher.

Auch im ‘beat calculator’ können Sie mit ‘O’ die Dateiliste anzeigen lassen. Markieren Sie dort den Song, dessen Tempo Sie bestimmen möchten und klicken Sie dann auf den Button ‘=>’. Der Song wird dann geladen (auch wenn möglicherweise der Name nicht im Feld erscheint). Der Ladevorgang benötigt übrigens einige Zeit, da der Song ganz in den Speicher geladen wird. Mit der mittleren Maustaste können Sie einen Zeitpunkt in der Sample-Darstellung des Songs markieren. Wenn Sie dann auf ‘Play’ klicken, wird die Wiedergabe von diesem Punkt gestartet. Wenn Sie nur einen Bereich wiedergeben möchten, können Sie diesen ebenfalls mit der mittleren Maustaste selektieren.

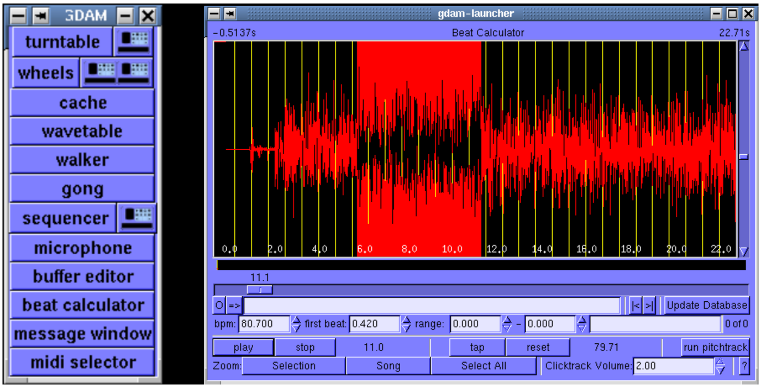


Abbildung 6.5: *Der GDAM-launcher (links). Im Fenster „Beat Calculator" kann das Tempo bestimmt werden.*

Es ist nicht möglich, das Tempo automatisch zu bestimmen. Seine manuelle Bestimmung ist aber sehr einfach. Klicken Sie während der Wiedergabe im Takt der Musik auf 'tap'. Die Zahl, die rechts neben dem 'Reset'-Button angezeigt wird, gibt das aus Ihren Mausklicks bestimmte Tempo an. Wenn Sie mit der Tempobestimmung fertig sind, können Sie diese Zahl in das Feld 'bpm' eintragen. Erhöhen Sie nun den Wert 'Clicktrack Volume' auf 2 und starten Sie die Wiedergabe erneut. Sie hören dann Song und Metronom. Wenn die Metronomschläge relativ zum Song verschoben sind, können Sie das in dem Feld 'first beat' (auch während der Wiedergabe) korrigieren.

Falls der Song mehrere Tempi aufweist, können Sie die Tempoangaben mit den 'range'-Feldern in Bereiche unterteilen. Im Eingabefeld neben den 'range'-Feldern können Sie dem Bereich einen Namen geben. Rechts davon befindet sich die Anzeige für die Anzahl der Bereiche und den gerade aktiven Bereich. Sie können neue Bereiche erzeugen, indem Sie auf die rechte der zwei Zahlen klicken. Wenn Sie auf die linke Zahl klicken, können Sie einen bestimmten Bereich aktivieren. Durch Klick mit der rechten Maustaste auf die rechte Zahl können Sie die Zahl der Bereiche um eins verringern. (Das geht jeweils nur einmal. Wenn Sie mehr als einen Bereich löschen möchten, müssen Sie vorher auf die linke Zahl klicken.)

Wenn Sie auf 'Update Database' klicken, werden Ihre Tempoangaben gespeichert. Die Angaben werden sofort in den 'Song Selector' übernommen. Wenn Sie mehrere Bereiche mit Tempoangaben versehen haben, können Sie sich dort diese Informationen mit 'info' anzeigen lassen. Vergessen Sie nicht, Ihre Songdatenbank im 'Song Selector' mit 'Save' zu speichern.

terminatorX – Ein effektvolles Programm – nicht nur zum Scratchen

Konfiguration des Programms

Bei terminatorX empfiehlt es sich, zunächst die Einstellungen für das Buffering zu überprüfen. Rufen Sie dazu mit dem Button 'Options' die entsprechende Dialogbox auf. Wenn Sie bei den Einstellungen für die Puffergröße die Zahl n einstellen, beträgt die tatsächliche Größe des Puffers 2^n. Um zunächst sicherzustellen, dass bei der Wiedergabe keine Klicks auftreten (auch dann nicht, wenn man während des Abspielens neue Musiktitel nachlädt), können Sie für die Größe des Puffers und die Anzahl der Puffer die Maximalwerte einstellen. Diese Werte werden in der Datei `.terminatorX3rc.bin` in Ihrem Home-Verzeichnis gespeichert. Bei diesen Werten ist allerdings die Reaktion des Programms auf Änderungen der Lautstärke- und Effekteinstellungen sehr langsam. Sie können auf Ihrem System mit den Einstellungen experimentieren und die kleinsten Werte herausfinden, bei denen keine Klicks auftreten. Bitte beachten Sie, dass auch Klicks und Verzerrungen auftreten können, wenn die Lautstärke übersteuert wird.

Um eine unterbrechungsfreie Wiedergabe auch bei kleineren Puffergrößen zu erzielen, können Sie das Programm auch mit Echtzeit-Priorität laufen lassen. Mehr dazu erfahren Sie im Abschnitt „Buffering und Latenzen" im Referenzhandbuch (als Besitzer einer **Personal Edition** finden Sie dieses auf den CDs, siehe Hinweis am Anfang des Kapitels).

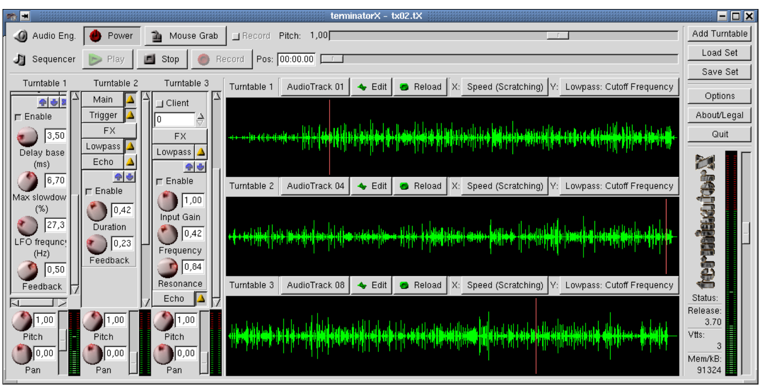


Abbildung 6.6: *Die Oberfläche von terminatorX*

Die Turntables und ihre Steuerkonsole

Bei terminatorX können Sie gleichzeitig mehrere „Turntables“ öffnen. Ein neuer „Turntable“ wird mit dem Button ‘Add Turntable’ hinzugefügt. Jeder „Turntable“ besitzt im linken Teil der Programmoberfläche eine eigene Steuerkonsole. Diese Konsolen sind in die Abschnitte ‘Main’, ‘Trigger’, ‘Lowpass’ und ‘Echo’ unterteilt. Außerdem gibt es einen Button ‘FX’ und Regler für Lautstärke und Tonhöhe (‘Pitch’). Mit dem Button ‘FX’ lassen sich unzählige Effekte in Form von LADSPA-Plugins in die Konsole einfügen.

Die einzelnen Abschnitte der Steuerkonsolen können durch Klick auf das entsprechende gelbe Dreieck geöffnet und verdeckt werden. Im Abschnitt ‘Main’ können Sie dem „Turntable“ einen Namen geben. Wenn die „Audio Engine“ gestoppt ist, können Sie den Turntable mit dem Button ‘Delete’ entfernen.

Im Abschnitt ‘Trigger’ können Sie Einstellungen dafür vornehmen, wann das Abspielen in einem bestimmten „Turntable“ beginnen soll. Mit dem Button ‘Trigger!’ können Sie die Wiedergabe sofort starten. Dies setzt allerdings voraus, dass die „Audio Engine“ bereits läuft. Wenn der Checkbutton ‘Auto’ aktiviert ist, wird die Wiedergabe für diesen „Turntable“ automatisch beim Start der „Audio Engine“ gestartet.

Musikdateien laden und abspielen

Nun wird es Zeit, dass wir anfangen Musik zu spielen und Musik-Dateien in die „Turntables“ laden. Klicken Sie dazu auf den Button, der sich oberhalb der schwarzen Anzeigefläche für die Sample-Daten links neben dem ‘Edit’-Button befindet. Wenn kein Lied geladen ist, ist dieser Button mit ‘NONE’ beschriftet. Es wird damit ein Filebrowser geöffnet, in dem Sie eine MP3 oder WAV-Datei auswählen können. Wenn die „Audio Engine“ läuft, wird bei einem einfachen Mausklick die angeklickte Datei sofort gespielt, und zwar unabhängig von der Mixer-Einstellung für diesen Kanal. Wenn man das vermeiden möchte, muss man die gewünschte Datei durch Doppelklick laden. Dieses Verhalten lässt sich im Menü ‘Options’ mit dem Checkbutton ‘Pre-Listen to audio files’ ausschalten. terminatorX lädt Musikdateien immer ganz in den Speicher, wobei MP3-Dateien entpackt werden. Das Programm benötigt daher relativ viel Speicher. Der vom Programm und den Musikdaten belegte Speicher wird links vom Master Volume-Regler angezeigt.

Hinweis

Sollte der vorhandene Speicher nicht ausreichen, wird auf die Festplatte ausgelagert. Dies führt normalerweise zu Störgeräuschen bei der Wiedergabe.

Hinweis

Die „Audio Engine“ wird durch Klick auf den ‘Power’-Button ein- und ausgeschaltet. Die Buttons ‘Play’, ‘Stop’ und Record beziehen sich auf den Sequenzer. Mit dem Sequenzer können sämtliche Mixer- und Effekt-Einstellungen dynamisch, d. h. zusammen mit ihrem zeitlichen Ablauf, gespeichert werden.

Wenn Sie eine Sequenz aufnehmen möchten, müssen Sie zuerst den Button ‘Record’ anklicken und die Aufnahme dann mit ‘Play’ starten. Wenn Sie die Aufnahme mit ‘Stop’ beendet haben, können Sie die Sequenz und sämtliche anderen Einstellungen mit ‘Save Set’ speichern. Wenn Sie ein gespeichertes „Set“ mit ‘Load Set’ laden, müssen Sie darauf achten, dass die Dateiendung `.tX` korrekt eingegeben wurde.

Falls terminatorX mit `root`-Privilegien läuft, können Sie in den ‘Mouse Grab’-Modus wechseln. Oberhalb jedes „Turntable“ befinden sich Auswahlbuttons, mit denen Sie den X- und Y-Koordinaten der Maus bestimmte Parameter zuordnen können. Der ‘Mouse Grab’-Modus wird mit (ESC) beendet.

Weitere Informationen zu terminatorX finden Sie im Verzeichnis `/usr/share/doc/packages/terminatorX` wahlweise im HTML oder Postscript-Format. Lesen Sie bitte auch die Datei `README.SuSE` in diesem Verzeichnis.

Hotplug

Mittlerweile werden in vielen Computern Hardwarekomponenten verwendet, die zur Laufzeit des Systems angeschlossen und wieder abgenommen werden können. Neben USB, als bekanntestes Beispiel für diese Komponenten, gibt es auch noch PCI, PCMCIA, Firewire, SCSI und andere Schnittstellen.

Hotplug-Systeme haben die Aufgabe, neue angeschlossene bzw. eingebaute Hardware zu erkennen und diese automatisch betriebsbereit einzurichten. Des Weiteren müssen Komponenten, die wieder entnommen werden sollen, auf diese Entnahme vorbereitet werden bzw. Ressourcen wieder frei gegeben werden, wenn Komponenten ohne Vorwarnung entfernt wurden.

Realisierung von Hotplug in Linux 144
Hotplug starten und Coldplug 144
USB 145
PCI und PCMCIA 147
Netzwerk 147
Firewire (IEEE1394) 148
Sonstige Geräte und weitere Entwicklung 149

Realisierung von Hotplug in Linux

Für gewöhnlich überwachen so genannte Daemonen Teile eines Systems auf externe Ereignisse, so überwacht z. B. der inetd eingehende Netzwerkanfragen. Der Daemon bei Hotplug ist der Kernel selbst. Dazu müssen die Treiber eines Busses in der Lage sein, neue Geräte zu erkennen und diese auf einheitlichen Weg dem System mitzuteilen. Im Kernel 2.4 sind USB, PCMCIA, Firewire, teilweise PCI und das Netzwerksubsystem dazu in der Lage. Dieser Teil von Hotplug ist in den jeweiligen Modulen fest eingebaut und lässt sich ohne Kerneländerung nicht weiter beeinflussen.

Hinweis

PCMCIA-Geräte werden nur dann von Hotplug behandelt, wenn diese CardBus-Karten sind und das Kernel PCMCIA-System gewählt wurde. Sie erscheinen dann als PCI-Geräte. Genauere Information finden Sie dazu im Abschnitt über PCMCIA.

Hinweis

Der zweite Teil von Hotplug leitet die notwendigen Schritte zum Einbinden von Geräten bzw. deren herauslösen ein und ist eine Sammlung von Skripten im Verzeichnis `/etc/hotplug` mit dem zentralen Script `/sbin/hotplug`. Dieses Skript ist die Schnittstelle zwischen dem Kernel und der Hotplug-Scriptsammlung.
Im weiteren Verlauf des Kapitels werden wir mit „Hotplug-System" diese Skripte bezeichnen.

Wenn ein hotplugfähiges Gerät angeschlossen oder entfernt wird, ruft der Kernel das Skript `/sbin/hotplug` auf und übergibt zusätzliche Informationen über die entsprechende Hardwarekomponente. Dieses Skript verteilt die Arbeit – je nach Art der Hardware – an weitere Skripte. Diese laden bzw. entladen die Kernelmodule und rufen wiederum weitere Programme zur Konfiguration der Komponenten auf. Die Programme liegen in `/etc/hotplug` und enden immer mit `.agent`.

Hotplug starten und Coldplug

Obwohl der Kernel immer Hotplugereignisse an `/sbin/hotplug` weitergibt, muss das Hotplug-System erst einmal gestartet werden. Solange Hotplug nicht gestartet ist, werden alle entsprechenden Ereignisse verworfen.

Außerdem gibt es Komponenten, die vom Kernel schon erkannt werden bevor überhaupt ein Zugriff auf das Dateisystem möglich ist. Diese Ereignisse

gehen einfach verloren. Deshalb wird in den Skripten `/etc/hotplug/*.rc` versucht, für bereits vorhandene Hardware diese Ereignisse künstlich zu erzeugen. In diesem Zusammenhang wird auch von „Coldplug“ gesprochen.

Falls zu diesem Zeitpunkt die USB-Basismodule noch nicht geladen sind, werden diese geladen und das USB-Gerätedateisystem (`usbdevfs`) eingehängt.

Wird Hotplug durch einen Aufruf von `rchotplug stop` angehalten, werden keine weiteren Ereignisse mehr ausgewertet. Wer nie während des Betriebs seine Hardware verändert, kann Hotplug auch vollständig deaktivieren. Allerdings muss dann auf andere Art und Weise für die Einrichtung von USB- oder PCMCIA-Geräten gesorgt werden.

Im Verzeichnis `/etc/sysconfig/hotplug` gibt es einige Variablen, die das Verhalten von Hotplug steuern. So kann z. B. mit der Variable ⟨*HOTPLUG_DEBUG*⟩ die „Gesprächigkeit“ von Hotplug beeinflusst werden. Über die Variablen ⟨*HOTPLUG_START_USB*⟩, ⟨*HOTPLUG_START_PCI*⟩ und ⟨*HOTPLUG_START_NET*⟩ kann eingestellt werden, dass nur Ereignisse bestimmten Typs verarbeitet werden. Alle weiteren Variablen sind in den entsprechenden Unterabschnitten näher erläutert.

Alle Meldungen von Hotplug werden immer in der Datei (`/var/log/messages`) (Systemlog) protokolliert.

USB

Wenn ein neues USB-Gerät angeschlossen wird, ermittelt das Skript `/etc/hotplug/usb.agent` einen geeigneten Treiber und stellt sicher, dass dieser geladen ist. Dieser Treiber muss nicht unbedingt ein Kernelmodul sein, so werden viele USB Kameras direkt von Anwendungsprogrammen angesprochen.

Die Zuordnung von Treibern zur Hardware ist mehrstufig: Als Erstes wird in der Datei `/etc/hotplug/usb.usermap` nachgesehen, ob diese Hardware von einem Anwendungsprogramm bzw. einem speziellen Initialisierungsskript bedient werden soll. Falls das nicht zutrifft, wird in `/etc/hotplug/usb.handmap` nach einer individuellen Zuordnung zu einem Kernelmodul gesucht. Wenn auch dort nichts gefunden wurde (was in den meisten Fällen zutrifft), wird letztendlich die Zuordnungstabelle des Kernels `/lib/modules/`⟨*kernelversion*⟩`/modules.usbmap` befragt. Des Weiteren wird hier nochmal ein USB-Hardwarescan durchgeführt, der bei der Verwendung von KDE als grafische Oberfläche weitere Aktionen auslöst. Zum Beispiel

wird für Geräte, die zum ersten Mal verwendet werden, ein geeignetes YaST-Modul zur Konfiguration angeboten oder Applikationen zur Verwendung mit dem neuen Gerät werden gestartet. Dieser Mechanismus läuft parallel zu den anderen Aktionen, die von `/etc/hotplug/usb.agent` ausgelöst werden.

USB-Geräte werden vom usb.agent je nach Typ unterschiedlich behandelt:

Speichergeräte wie z. B. Festplatten werden vom Skript path/usr/sbin/checkhotmounts behandelt, sobald die erforderlichen Treiber geladen sind.

Netzwerkgeräte erzeugen ein eigenes Hotplugereignis im Kernel, sobald diese registriert werden. Der `usb.agent` hinterlegt lediglich Hardwareinformationen, die später vom Netzwerkereignis verwendet werden. Dies ist nur eine vorübergehende Lösung für den Kernel 2.4 und versagt, wenn mehrere USB-Netzwerkgeräte verwendet werden. Dies kommt jedoch nur sehr selten vor.

Kameras werden über den Hardwarescan/KDE-Mechanismus angesprochen. Dazu werden allerdings noch via `/etc/hotplug/usb/usbcam` die Zugriffsrechte der Gerätedatei für den eingeloggten Benutzer gesetzt, damit dieser unter KDE darauf zugreifen kann.

Mäuse benötigen nur ein geladenes Modul, welches hier geladen wird, um sofort verwendet zu werden.

Tastaturen werden schon beim Bootvorgang benötigt und werden deshalb nicht von Hotplug behandelt.

ISDN/Modem wird derzeit noch nicht automatisch eingerichtet.

Es gibt noch einige USB-spezifische Variablen in `/etc/sysconfig/hotplug`. In ⟨*HOTPLUG_USB_HOSTCONTROLLER_LIST*⟩ stehen die Treiber für den USB-Controller in der Reihenfolge, wie sie zu laden versucht werden. Wird ein Treiber erfolgreich geladen, werden in ⟨*HOTPLUG_USB_MODULES_TO_UNLOAD*⟩ die Module eingetragen, die beim Entfernen der Komponente wieder entladen werden sollen. Alle nachfolgenden Module für USB werden nicht entladen, weil nicht sicher entschieden werden kann, ob sie noch von einem Gerät benötigt werden. Die Variable ⟨*HOTPLUG_USB_NET_MODULES*⟩ enthält die Namen der Module, die ein Netzwerkinterface zur Verfügung stellen. Sobald eines dieser Module geladen wird, wird eine Hardwarebeschreibung zur späteren Verwendung beim Netzwerkereignis abgelegt. Dieser Vorgang wird im Systemlog protokolliert.

PCI und PCMCIA

Bei PCMCIA-Karten muss sorgfältig unterschieden werden, da außer CardBus-Karten keine PC-Carten von Hotplug behandelt werden; diese wiederum auch nur dann, wenn das Kernel PCMCIA-System aktiv ist. Dieser Sachverhalt wird im PCMCIA-Kapitel im Abschnitt Software (xxPCMCIA-SOFTWARExx) genauer erklärt.

CardBus-Karten sind technisch gesehen beinahe PCI-Geräte. Deshalb werden beide von demselben Hotplug-Skript `/etc/hotplug/pci.agent` behandelt. Dort wird im Wesentlichen ein Treiber für die Karte ermittelt und geladen. Außerdem wird eine Information darüber, wo die neue Karte angeschlossen wurde (PCI-Bus/PCMCIA-Slots und die Slotnummer) abgelegt, damit ein nachfolgendes Hotplug-Netzwerk-Ereignis diese Information lesen und die richtige Konfiguration auswählen kann.

Die Treiberzuordnung ist hier zweistufig: Zuerst wird in der Datei `/etc/hotplug/pci.handmap` nach individuellen Einstellungen gesucht und falls nichts gefunden wurde, wird in der PCI-Treibertabelle des Kernels `/lib/modules/`⟨*kernelversion*⟩`/modules.pcimap` gesucht. Wer also die Treiberzuordnung verändern möchte, sollte dazu `/etc/hotplug/pci.handmap` anpassen, da die andere Tabelle bei einem Kernelupdate überschrieben wird.

Anders als bei USB werden keine besonderen Aktionen je nach Art der PCI- oder CardBus-Karte ausgeführt. Bei Netzwerkkarten erzeugt der Kernel ein Hotplug-Netzwerkereignis, das die Einrichtung des Interfaces veranlasst. Bei allen anderen Karten müssen weitere Aktionen manuell ausgeführt werden. Das Hotplug-System wird aber diesbezüglich noch erweitert.

Sobald die Karte entfernt wird, werden auch die verwendeten Module wieder entladen. Falls das Entfernen bei bestimmten Modulen zu Problemen führt, kann dies verhindert werden, indem die Modulnamen in `/etc/sysconfig/hotplug` in die Variable ⟨*HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD*⟩ geschrieben werden.

Netzwerk

Sobald im Kernel ein neues Netzwerkinterface an- oder abgemeldet wird, erzeugt dieser ein Hotplug-Netzwerkereignis. Dieses wird von `/etc/hotplug/net.agent` ausgewertet. Gegenwärtig werden dort nur Ethernet-, Tokenring- und WirelessLAN-Interfaces berücksichtigt. Für alle anderen Arten von Netzwerken wie Modem oder ISDN gibt es andere Mechanismen. Auch Netzwerkinterfaces, die von PCMCIA-Karten bereitgestellt werden und

nicht von Hotplug, sondern vom Cardmanager behandelt werden, werden hier nicht behandelt. Es erscheint dann eine entsprechende Meldung im Systemlog.

Zuerst wird zu ermitteln versucht, welche Hardware das Interface bereitstellt. Da der Kernel 2.4 solche Information nicht liefern kann, wird eine Information verwendet, die bei dem vorangegangenen USB- oder PCI-Hotplug-Ereignis bereitgestellt wurde. Obwohl dies in den meisten Fällen gut funktioniert, ist es als vorübergehende Notlösung zu betrachten. Es dürfen deswegen nämlich nicht zwei Netzwerkkarten gleichzeitig angeschlossen werden. Sollten Sie mehrere hotplugfähige Netzwerkkarten verwenden, dann verbinden Sie diese bitte nacheinander mit dem Computer. Ein zeitlicher Abstand von wenigen Sekunden genügt. Diese Informationsübermittlung wird in `/var/log/messages` protokolliert.

Mit dieser Information über die zugrunde liegende Hardware wird dann das Skript `/sbin/ifup` (bzw. `ifdown`) aufgerufen. ifup ist so in der Lage, einer bestimmten Karte immer die richtige Konfiguration zuzuweisen, auch wenn das Interface einen anderen Namen hat. Interfacenamen werden vom Kernel nämlich nicht gezielt zugeordnet.

Weitere individuelle Aktionen, die Sie ausführen lassen möchten, nachdem ein neues Netzwerkinterface angelegt wurde, können Sie in `/sbin/ifup` einhängen. Details dazu finden sich in der Manpage zu Manual-Page von `ifup` (`man ifup`). Es ist auch möglich, je nach angeschlossener Hardware unterschiedliche Defaultrouten zu verwenden; siehe dazu Manual-Page von `route` (`man route`).

Falls die automatische Ermittlung der Hardware hinter dem Interface fehlschlägt (z. B. bei Firewire) und nur ein hotplugfähiges Netzwerkgerät verwendet wird, dann kann die Beschreibung der Netzwerkhardware in `/etc/sysconfig/hotplug` in die Variable ⟨*HOTPLUG_NET_DEFAULT_HARDWARE*⟩ geschrieben werden. Diese Zeichenkette muss dem entsprechen, was von `/sbin/ifup` zur Zuordnung der richtigen Konfiguration verwendet werden soll. In der Variable ⟨*HOTPLUG_NET_TIMEOUT*⟩ wird festgelegt, wie lange `net.agent` auf eine dynamisch erzeugte Hardwarebeschreibung wartet.

Firewire (IEEE1394)

Für Firewire-Geräte werden derzeit nur die Treibermodule geladen. Um einen Überblick zu bekommen, wie stark Firewire-Hardware unter unseren Kunden verbreitet ist, können Sie uns über unser Feedback-Webfrontend `http://www.suse.de/feedback` kontaktieren.

Sonstige Geräte und weitere Entwicklung

Alle hier nicht beschriebenen Arten von hotplugfähiger Hardware werden gegenwärtig (noch) nicht behandelt. Hotplug unterliegt aber zur Zeit einer starken Entwicklung, die jedoch sehr von den Fähigkeiten des Kernels abhängt. Es ist zu erwarten, dass zusammen mit dem nächsten Kernel 2.6 wesentlich bessere Möglichkeiten geboten werden.

Konfiguration und mobiles Arbeiten mit Notebooks

An Notebooks werden besondere Anforderungen gestellt. Hierzu zählen unter anderem Power Management (APM/ACPI), Infrarot-Schnittstellen (IrDA) und PC-Karten (PCMCIA). Gelegentlich sind auch in Desktop-Rechnern solche Komponenten zu finden; sie unterscheiden sich nur unwesentlich von den in Notebooks verwendeten Spezifika – deshalb wird deren Verwendung und Konfiguration in diesem Kapitel zusammengefasst.

PCMCIA 152
SCPM – System Configuration Profile Management 164
APM und ACPI – Powermanagement 171
IrDA – Infrared Data Association 178

PCMCIA

PCMCIA steht für „Personal Computer Memory Card International Association“ und wird als Sammelbegriff für sämtliche damit zusammenhängende Hard- und Software verwendet.

Die Hardware

Die wesentliche Komponente ist die PCMCIA-Karte; hierbei unterscheidet man zwei Typen:

PC-Karten Das sind die derzeit noch am häufigsten vorkommenden Karten. Sie verwenden einen 16 Bit breiten Bus zur Datenübertragung, sind meist relativ günstig und werden i. d. R. problemlos und stabil unterstützt.

CardBus-Karten Dies ist eine neuerer Standard. Sie verwenden einen 32 Bit breiten Bus, sind dadurch schneller, aber auch teurer. Da die Datenübertragungsrate aber häufig an anderer Stelle eingeschränkt wird, lohnt sich der Aufwand häufig nicht. Es gibt mittlerweile auch für diese Karten etliche Treiber, wobei manche immer noch instabil sind – abhängig auch vom vorhandenen PCMCIA-Controller.

Welche Karte eingeschoben ist, sagt bei aktivem PCMCIA-Dienst das Kommando `cardctl ident`. Eine Liste von unterstützten Karten findet man in `SUPPORTED\_CARDS` in `/usr/share/doc/packages/pcmcia`. Dort gibt es auch die jeweils aktuelle Version des PCMCIA-HOWTO.

Die zweite notwendige Komponente ist der PCMCIA-Controller, oder auch die PC-Card/CardBus-Bridge. Diese stellt die Verbindung zwischen der Karte und dem PCI-Bus her, in älteren Geräten auch die Verbindung zum ISA-Bus. Diese Controller sind fast immer zu dem Intel-Chip i82365 kompatibel; es werden alle gängigen Modelle unterstützt. Der Typ des Controllers lässt sich mit dem Kommando `probe` ermitteln. Falls es ein PCI-Gerät ist, liefert auch das Kommando `lspci -vt` interessante Informationen.

Die Software

Unterschiede zwischen den beiden existierenden PCMCIA-Systemen

Gegenwärtig gibt es zwei PCMCIA Systeme, externes PCMCIA und Kernel-PCMCIA. Das externe PCMCIA System von David Hinds ist das ältere, somit

auch besser erprobte und wird immer noch weiterentwickelt. Die Quellen der verwendeten Module sind nicht in die Kernelquellen integriert, deshalb „externes“ System. Seit Kernel 2.4 gibt es alternative Module in den Kernelquellen. Diese bilden das Kernel PCMCIA System. Die Basismodule wurden von Linus Torvalds geschrieben und unterstützen vor allem neuere CardBus Bridges besser.

Leider sind diese beiden Systeme zueinander inkompatibel. Außerdem gibt es in beiden Systemen unterschiedliche Sätze von Kartentreibern. Deswegen kommt je nach verwendeter Hardware nur ein System in Frage. Die Voreinstellung in SuSE Linux ist das neuere Kernel PCMCIA. Es ist jedoch möglich, das System zu wechseln. Dazu muss in der Datei `/etc/sysconfig/pcmcia` der Variablen ⟨*PCMCIA_SYSTEM*⟩ entweder `external` oder `kernel` zugewiesen und PCMCIA mit `rcpcmcia restart` neu gestartet werden. Für vorübergehende Wechsel können Sie auch `rcpcmcia [re]start external,kernel` verwenden. Detailinformationen dazu befindet sich in `/usr/share/doc/packages/pcmcia/LIESMICH.SuSE`

Die Basismodule

Die Kernelmodule für beide Systeme befinden sich in den Kernelpaketen. Zusätzlich werden noch die Paket `pcmcia` und `hotplug` benötigt.

Beim Start von PCMCIA werden die Module `pcmcia_core`, `i82365` (externes PCMCIA) oder `yenta_socket` (Kernel-PCMCIA) und `ds` geladen. In sehr seltenen Fällen wird alternativ zu `i82365` bzw. `yenta_socket` das Modul `tcic` benötigt. Sie initialisieren die vorhandenen PCMCIA-Controller und stellen Basisfunktionen zur Verfügung.

Der Cardmanager

Da PCMCIA-Karten zur Laufzeit gewechselt werden können, muss es einen Daemonen geben, der die Aktivitäten in den Steckplätzen überwacht. Diese Aufgabe erledigen je nach gewähltem PCMCIA System und verwendeter Hardware der Cardmanager oder das Hotplug System des Kernels. Bei externem PCMCIA kommt nur der Cardmanager zum Einsatz. Bei Kernel-PCMCIA handhabt der Cardmanager nur die PC-Card Karten, wohingegen CardBus Karten von Hotplug behandelt werden. Der Cardmanager wird vom PCMCIA Startskript nach dem Laden der Basismodule gestartet. Da Hotplug neben PCMCIA auch noch andere Subsysteme bedient, gibt es hierfür ein eigenes Startskript. (Siehe auch Kapitel *Hotplug* auf Seite 143).

Ist eine Karte eingeschoben, ermittelt der Cardmanager bzw. Hotplug Typ und Funktion und lädt die passenden Module. Wurden diese erfolgreich

geladen, startet der Cardmanager bzw. Hotplug je nach Funktion der Karte bestimmte Initialisierungsskripten, die ihrerseits die Netzwerkverbindung aufbauen, Partitionen von externen SCSI-Platten einhängen (mounten) oder andere hardwarespezifische Aktionen ausführen. Die Scripte des Cardmanager befinden sich in `/etc/pcmcia`. Die Scripte für Hotplug sind in `/etc/hotplug` zu finden. Wenn die Karte wieder entfernt wird, beendet der Cardmanager bzw. Hotplug mit den selben Skripten die diversen Kartenaktivitäten. Anschließend werden die nicht mehr benötigten Module wieder entladen.

Sowohl der Startvorgang von PCMCIA als auch die Kartenereignisse werden im Systemlog (`/var/log/messages`) protokolliert. Dort wird festgehalten, welches PCMCIA System gerade verwendet wird und welcher Daemon welche Scripte zur Einrichtung verwendet hat. Theoretisch kann eine PCMCIA Karte einfach entnommen werden. Dies funktioniert auch hervorragend für Netzwerk-, Modem- oder ISDN-Karten, solange keine aktiven Netzwerkverbindungen mehr bestehen. Es funktioniert nicht im Zusammenhang mit eingehängten Partitionen einer externen Platte oder mit NFS-Verzeichnissen. Hier müssen Sie dafür sorgen, dass die Einheiten synchronisiert und sauber ausgehängt werden (unmounten). Das ist natürlich nicht mehr möglich, wenn die Karte bereits gezogen wurde. Im Zweifelsfall hilft ein

```
cardctl eject
```

Dieser Befehl deaktiviert alle Karten, die sich noch im Notebook befinden. Um nur eine der Karten zu deaktivieren, können Sie zusätzlich die Slotnummer angeben, z. B. `cardctl eject 0`.

Die Konfiguration

Ob PCMCIA bzw. Hotplug beim Booten gestartet wird, lässt sich mit dem YaST2 Runleveleditor oder auf der Kommandozeile mittels `chkconfig` einstellen .

In `/etc/sysconfig/pcmcia` befinden sich vier Variablen:

⟨***PCMCIA_SYSTEM***⟩ bestimmt, welches PCMCIA System verwendet wird.

⟨***PCMCIA_PCIC***⟩ enthält den Namen des Moduls, das den PCMCIA-Controller ansteuert. Im Normalfall ermittelt das Startskript diesen Namen selbstständig. Nur wenn dies fehlschlägt, kann das Modul hier eingetragen werden. Ansonsten sollte diese Variable leer bleiben.

⟨*PCMCIA_CORE_OPTS*⟩ ist für Parameter für das Modul pcmcia_core gedacht; sie werden aber nur selten benötigt. Diese Optionen sind in Manual-Page von pcmcia_core (man pcmcia_core) beschrieben.

⟨*PCMCIA_PCIC_OPTS*⟩ nimmt Parameter für das Modul i82365 auf. Auch hierzu gibt es eine Manpage Manual-Page von i82365 (man i82365). Falls yenta_socket verwendet wird, werden diese Optionen ignoriert, da yenta_socket keine Optionen kennt.

Die Zuordnung von Treibern zu PCMCIA Karten für den Cardmanager befindet sich in den Dateien /etc/pcmcia/config und /etc/pcmcia/*.conf. Zuerst wird config gelesen und dann die *.conf in alphabetischer Reihenfolge. Der zuletzt gefundene Eintrag für eine Karte ist ausschlaggebend. Details über die Syntax dieser Dateien befinden sich in der Manual-Page von pcmcia (man pcmcia).

Die Zuordnung von Treibern zu PCMCIA Karten für Hotplug wird im Kapitel über Hotplug beschrieben (siehe *Hotplug* auf Seite 143).

Netzwerkkarten (Ethernet, Wireless LAN und TokenRing)

Diese lassen sich wie gewöhnliche Netzwerkkarten mit YaST2 einrichten. Dort muss lediglich 'PCMCIA' als Kartentyp ausgewählt werden. Alle weiteren Details zur Netzwerkeinrichtung befinden sich im Netzwerkkapitel. Beachten Sie dort die Hinweise zu hotplugfähigen Karten.

ISDN

Auch bei ISDN-PC-Karten erfolgt die Konfiguration größtenteils wie bei sonstigen ISDN-Karten mit YaST2. Es spielt keine Rolle welche der dort angebotenen PCMCIA ISDN-Karten ausgewählt wird; wichtig ist nur, das es eine PCMCIA Karte ist. Bei der Einrichtung der Hardware und der Provider ist darauf zu achten, dass der Betriebsmodus immer auf hotplug, nicht auf onboot steht.

So genannte ISDN-Modems gibt es auch bei PCMCIA-Karten. Dies sind, Modem- oder Multifunktionskarten mit einem zusätzlichen ISDN-Connection-Kit und werden wie ein Modem behandelt.

Modem

Bei Modem-PC-Karten gibt es im Normalfall keine PCMCIA-spezifischen Einstellungen. Sobald ein Modem eingeschoben wird, steht dieses unter /dev/modem zur Verfügung.

Es gibt auch bei PCMCIA Karten so genannte Softmodems. Diese werden i. d. R. nicht unterstützt. Falls es irgendwelche Treiber gibt, müssen diese individuell ins System eingebunden werden.

SCSI und IDE

Das passende Treibermodul wird vom Cardmanager oder Hotplug geladen. Sobald also eine SCSI- oder IDE-Karte eingeschoben wird, stehen die daran angeschlossenen Geräte zur Verfügung. Die Gerätenamen werden dynamisch ermittelt. Informationen über vorhandene SCSI- bzw. IDE- Geräte sind unter `/proc/scsi` bzw. unter `/proc/ide` zu finden.

Externe Festplatten, CD-ROM-Laufwerke und ähnliche Geräte müssen eingeschaltet sein, bevor die PCMCIA-Karte in den Steckplatz eingeschoben wird. SCSI-Geräte müssen aktiv terminiert werden.

Hinweis

Bevor eine SCSI- oder IDE-Karte entnommen wird, müssen sämtliche Partitionen der daran angeschlossenen Geräte ausgehängt werden. Wurde dies vergessen, kann erst nach einem Reboot des Systems erneut auf diese Geräte zugegriffen werden, auch wenn der Rest des Systems durchaus stabil weiterläuft.

Hinweis

Sie können Linux auch vollständig auf solchen externen Platten installieren. Allerdings gestaltet sich dann der Bootvorgang etwas komplizierter. Es wird auf alle Fälle eine Bootdisk benötigt, die den Kernel und eine Init-Ramdisk (initrd) enthält; mehr Informationen dazu finden Sie in Abschnitt *Booten mit der initial ramdisk* auf Seite 202 . Die initrd enthält ein virtuelles Dateisystem, das alle benötigten PCMCIA-Module und -Programme enthält. Die Bootdisk bzw. die Bootdisk-Images sind ebenso aufgebaut, damit könnten Sie Ihre externe Installation immer booten. Es ist jedoch umständlich, jedes Mal die PCMCIA-Unterstützung von Hand zu laden. Fortgeschrittene Anwender können sich eine auf das jeweilige System zugeschnittene Bootdiskette selbst erstellen Hinweise finden Sie dazu in dem englischsprachigem PCMCIA-HOWTO in Abschnitt *5.3 Booting from a PCMCIA device*.

Konfigurationen zum Umschalten – SCPM

Häufig benötigt man bei mobilen Computern verschiedene Konfigurationsprofile, für Firma oder für zu Hause. Mit PCMCIA-Geräten war dies dank der PCMCIA Schemata noch nie ein Problem. Da jedoch auch Betreiber von

fest eingebauten Netzwerkkarten oder USB/FireWire Geräten verschiedene Profile für die Systemkonfiguration verwenden möchten, gibt es seit SuSE Linux 8.0 das Paket SCPM (System Configuration Profile Management). Deshalb unterstützt SuSE die PCMCIA Schemata nicht mehr. Wer diese dennoch verwenden möchte, muss die Konfiguration unter `/etc/pcmcia` von Hand anpassen. Wir empfehlen jedoch einen Umstieg auf SCPM, da sich damit beliebige Teile der Systemkonfiguration verwalten lassen, nicht nur PCMCIA bezogene.

Die Dokumentation zu SCPM befindet sich im Abschnitt *SCPM – System Configuration Profile Management* auf Seite 164.

Wenn's trotzdem nicht geht

Bisweilen kommt es bei der Verwendung von PCMCIA auf manchen Notebooks oder mit manchen Karten zu Problemen. Die meisten Schwierigkeiten lassen sich mit wenig Aufwand bewältigen, solange man die Sache systematisch angeht.

Achtung

Da es in SuSE Linux sowohl externes als auch Kernel PCMCIA nebeneinander gibt, muss beim manuellen Laden von Modulen eine Besonderheit beachtet werden. Die beiden PCMCIA Systeme verwenden Module gleichen Namens und sind in unterschiedlichen Unterverzeichnissen unter `/lib/modules/`⟨*kernelversion*⟩ untergebracht. Diese Unterverzeichnisse heißen `pcmcia` für Kernel-PCMCIA und `pcmcia-external` für externes PCMCIA. Deshalb muss beim manuellen Laden von Modulen dieses Unterverzeichnis angegeben werden, entweder mittels `insmod /lib/modules/`⟨*kernelversion*⟩/⟨*Unterverzeichnis*⟩/⟨*dateiname des Moduls*⟩ oder mit `modprobe -t` ⟨*Unterverzeichnis*⟩ ⟨*modulname*⟩.

Achtung

Zuerst ist herauszufinden, ob das Problem mit einer Karte zusammenhängt, oder ob ein Problem des PCMCIA-Basissystems vorliegt. Deshalb sollten Sie in jedem Fall den Computer zunächst ohne eingeschobene Karten starten. Erst wenn das Basissystem einwandfrei zu funktionieren scheint, wird die Karte eingeschoben. Alle aufschlussreichen Meldungen werden in `/var/log/messages` protokolliert. Deshalb sollte die Datei mit

```
tail -f /var/log/messages
```

während der notwendigen Tests beobachtet werden. So lässt sich der Fehler auf einen der beiden folgenden Fälle einschränken.

Das PCMCIA-Basissystem funktioniert nicht

Wenn das System beim Booten bereits bei der Meldung PCMCIA: "Starting services" stehen bleibt oder andere merkwürdige Dinge geschehen, kann das Starten von PCMCIA beim nächsten Booten durch die Eingabe von `NOPCMCIA=yes` am Bootprompt verhindert werden. Um den Fehler weiter einzugrenzen, werden nun die drei Basismodule des verwendeten PCMCIA Systems von Hand nacheinander geladen.

Dazu dienen die Kommandos

erde:~ # **modprobe -t ⟨*dir*⟩ pcmcia_core**

erde:~ # **modprobe -t pcmcia-external i82365** (bei externem PCMCIA) bzw.

erde:~ # **modprobe -t pcmcia yenta_socket** (bei kernel PCMCIA)

bzw. – in sehr seltenen Fällen –

erde:~ # **modprobe -t ⟨*dir*⟩ tcic**

und

erde:~ # **modprobe -t ⟨*dir*⟩ ds**

Die kritischen Module sind die beiden ersten.

Tritt der Fehler beim Laden von `pcmcia_core` auf, hilft die Manpage zu `pcmcia_core` weiter. Die darin beschriebenen Optionen können zunächst zusammen mit dem Kommando modprobe getestet werden. Als Beispiel können wir die APM Unterstützung der PCMCIA-Module abschalten; in wenigen Fällen kann es damit Probleme geben. Dafür gibt es die Option doapm; mit `do_apm=0` wird das Powermanagement deaktiviert:

modprobe -t ⟨*dir*⟩ pcmciacore do_apm=0

Führt die gewählte Option zum Erfolg, wird sie in der Datei `/etc/sysconfig/pcmcia` in die Variable ⟨*PCMCIA_CORE_OPTS*⟩ geschrieben:

```
PCMCIA_CORE_OPTS="do_apm=0"
```

Vereinzelt kann das Prüfen freier IO-Bereiche Ärger machen, wenn sich dadurch andere Hardwarekomponenten gestört fühlen. Das umgeht man dann mit `probe_io=0`. Sollen mehrere Optionen verwendet werden, müssen sie durch Leerzeichen getrennt werden:

```
PCMCIA_CORE_OPTS="do_apm=0 probe_io=0"
```

Wenn es beim Laden des Moduls `i82365` zu Fehlern kommt, hilft die Manpage zu Manual-Page von `i82365` (`man i82365`).

Ein Problem in diesem Zusammenhang ist ein Ressourcenkonflikt, ein Interrupt, IO-Port oder Speicherbereich wird doppelt belegt. Das Modul `i82365` prüft zwar diese Ressourcen, bevor sie für eine Karte zur Verfügung gestellt werden, jedoch führt manchmal genau diese Prüfung zum Problem. So führt das Prüfen des Interrupt 12 (PS/2-Geräte) bei manchen Computern zum Blockieren von Maus und/oder Tastatur. In diesem Fall hilft der Parameter `irq_list=`⟨*ListevonIRQs*⟩. Die Liste soll alle IRQs enthalten, die verwendet werden dürfen. Also

```
modprobe i82365 irq_list=5,7,9,10
```

oder dauerhaft in `/etc/sysconfig/pcmcia`:

```
PCMCIA_PCIC_OPTS="irq_list=5,7,9,10"
```

Weiterhin gibt es `/etc/pcmcia/config` und `/etc/pcmcia/config.opts`. Diese Dateien werden vom Cardmanager ausgewertet. Die darin gemachten Einstellungen sind erst für das Laden der Treiber-Module für die PCMCIA-Karten relevant. In `/etc/pcmcia/config.opts` können auch IRQs, IO-Ports und Speicherbereiche ein- oder ausgeschlossen werden. Der Unterschied zur Option irqlist ist, dass die in config.opts ausgeschlossenen Ressourcen zwar nicht für eine PCMCIA-Karte verwendet, aber dennoch vom Basis-Modul i82365 geprüft werden.

Die PCMCIA-Karte funktioniert nicht (richtig)

Hier gibt es im Wesentlichen drei Varianten: Die Karte wird nicht erkannt, der Treiber kann nicht geladen werden oder das Interface, das vom Treiber bereitgestellt wird, wird falsch eingerichtet.

Man sollte beachten, ob die Karte vom Cardmanager oder von hotplug behandelt wird. Nochmal zur Erinnerung: Bei externem PCMCIA regiert immer der Cardmanager, bei Kernel PCMCIA behandelt der Cardmanager PC-Card Karten und Hotplug behandelt CardBUS Karten. Hier wird nur der Cardmanager besprochen. Hotplug Probleme werden im Hotplug Kapitel behandelt (siehe Kapitel *Hotplug* auf Seite 143).

- **Die Karte wird nicht erkannt.**
  Wenn die Karte nicht erkannt wird, erscheint in `/var/log/messages` die Meldung "unsupported Card in Slot x". Diese Meldung besagt lediglich, dass der Cardmanager der Karte keinen Treiber zuordnen kann. Zu dieser Zuordnung wird `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` benötigt. Diese Dateien sind sozusagen die

Treiberdatenbank. Diese Treiberdatenbank lässt sich am leichtesten erweitern, wenn man vorhandene Einträge als Vorlage nimmt. Sie können mit dem Kommando `cardctl ident` herausfinden, wie die Karte sich identifiziert. Weitere Informationen dazu befinden sich im PCMCIA-HOWTO Abschnitt 6 und in der Manual-Page von `pcmcia` (`man pcmcia`). Nach der Änderung von `/etc/pcmcia/config` bzw. `/etc/pcmcia/*.conf` muss die Treiberzuordnung neu geladen werden; dazu genügt ein `rcpcmcia reload`.

- **Treiber wird nicht geladen**
  Eine Ursache hierfür besteht darin, dass in der Treiberdatenbank eine falsche Zuordnung gespeichert ist. Das kann z. B. daher kommen, dass ein Hersteller in ein äußerlich unverändertes Kartenmodell einen anderen Chip einbaut. Manchmal gibt es auch alternative Treiber, die bei bestimmten Modellen besser (oder überhaupt erst) funktionieren als der voreingestellte Treiber. In diesen Fällen werden genaue Informationen über die Karte benötigt. Hier hilft auch, eine Mailingliste oder den Advanced Support Service zu fragen.

  Eine weitere Ursache ist ein Ressourcenkonflikt. Bei den meisten PCMCIA-Karten ist es nicht relevant, mit welchem IRQ, IO-Port oder Speicherbereich sie betrieben werden, aber es gibt auch Ausnahmen. Dann sollte man zuerst immer nur eine Karte testen und evtl. auch andere Systemkomponenten wie z. B. Soundkarte, IrDA, Modem oder Drucker vorübergehend abschalten. Die Ressourcenverteilung des Systems kann man mit `lsdev` einsehen (Es ist durchaus normal, dass mehrere PCI Geräte denselben IRQ verwenden).

  Eine Lösungsmöglichkeit wäre. eine geeignete Option für das Modul `i82365` zu verwenden (siehe oben PCMCIA_PCIC_OPTS). Es gibt jedoch auch für manche Kartentreibermodule Optionen. Diese lassen sich mit `modinfo /lib/modules/`⟨*richtiges pcmcia Verzeichnis*⟩/⟨*treiber*⟩.o herausfinden (der vollständige Pfad ist hier wieder nötig, um den Treiber vom richtigen PCMCIA System anzusprechen). Für die meisten Module gibt es auch eine Manpage. Tipp: `rpm -ql pcmcia | grep man` listet alle im pcmcia enthaltene Manual-Pages auf. Zum Testen der Optionen können die Kartentreiber auch von Hand entladen werden. Hierbei ist wieder zu beachten, dass das Modul des gerade verwendeten PCMCIA Systems zu verwenden. Siehe die Warnung weiter oben.

  Wenn eine Lösung gefunden wurde, kann in `/etc/pcmcia/config.opts` die Verwendung einer bestimmten Ressource allgemein erlaubt bzw. verboten werden. Auch die Optionen für Kartentreiber finden hier Platz Soll z. B. das Modul `pcnet_cs` ausschließlich mit dem IRQ 5 be-

trieben werden, wird folgender Eintrag benötigt:

```
module pcnet_cs opts irq_list=5
```

Ein Problem, das manchmal mit 10/100-MBit-Netzwerkkarten auftritt: Die Übertragungsart wird nicht automatisch richtig erkannt. Hier hilft das Kommando `ifport` oder `mii_tool`. Damit lässt sich die eingestellte Übertragungsart anzeigen und verändern. Um diese Kommandos automatisch ausführen zu lassen, muss das Script `/etc/pcmcia/network` individuell angepasst werden.

- **Interface wird falsch konfiguriert**
  In diesem Fall ist es empfehlenswert, die Konfiguration des Interfaces nochmal genau zu überprüfen, um seltene Konfigurationsfehler auszuschließen. Bei Netzwerkkarten kann außerdem die Dialograte der Netzwerkskripten erhöht werden, in dem man in `/etc/sysconfig/network/config` der Variable `DEBUG=yes` zuweist. Bei anderen Karten, oder wenn das noch nicht hilft, gibt es noch die Möglichkeit, in das vom Cardmanager aufgerufene Script (siehe `/var/log/messages`) eine Zeile `set -x` einzubauen. Dadurch wird jedes einzelne Kommando des Scripts im Systemlog protokolliert. Hat man die kritische Stelle in einem Script gefunden, können die entsprechenden Kommandos auch in einem Terminal eingegeben und getestet werden.

Installation via PCMCIA

In manchen Fällen wird PCMCIA bereits zum Installieren benötigt, wenn man über Netzwerk installieren möchte oder das CD-ROM via PCMCIA betrieben wird. Dazu muss man mit einer Bootdiskette starten. Des weiteren wird eine der Moduldisketten benötigt.

Nach dem Booten von Diskette (oder auch nach der Auswahl 'manuelle Installation' beim Booten von CD) wird das Programm `linuxrc` gestartet. Dort muss unter dem Menüpunkt 'Kernel-Module (Hardware-Treiber)' der Punkt 'Lade PCMCIA Module' ausgewählt werden. Zuerst erscheinen zwei Eingabefelder, in denen man Optionen für die Module `pcmcia_core` und `i82365` eingeben kann. Im Normalfall bleiben diese Felder jedoch leer. Die Man-Pages für `pcmcia_core` und `i82365` befinden sich als Textdateien auf der ersten CD im Verzeichnis `docu`.

Nach dem aktuellen Stand der Entwicklung wird bei SuSE Linux 8.1 nach wie vor mit dem externen PCMCIA System installiert. Sollte sich dies nach Fertigstellung des Buches noch ändern, erkennen Sie das daran, dass keine Moduloptionen für `i82365` erfragt werden und stattdessen das Modul

yenta_socket verwendet wird. Während der Installation werden Systemmeldungen auf verschiedenen virtuellen Konsolen ausgegeben, auf die man mit Alt + Funktionstaste umschalten kann. Später, wenn bereits eine grafische Oberfläche aktiv ist, muss man Ctrl + Alt + Funktionstaste verwenden.

Es gibt auch schon während der Installation Terminals, auf denen Kommandos ausgeführt werden können. Solange linuxrc läuft, ist das die Konsole 9 (eine sehr spartanisch ausgestattete Shell); sobald das Installationssystem geladen ist (YaST2 wurde gestartet) gibt es auf Konsole 2 eine bash und viele gängige Systemtools.

Wenn während der Installation ein falsches Treibermodul für eine PCMCIA Karte geladen wird, muss die Bootdiskette von Hand angepasst werden. Dazu benötigt man jedoch fortgeschrittene Linuxkenntnisse. Wenn der erste Teil der Installation abgeschlossen ist, wird das System teilweise oder ganz neu gestartet. Dabei kann in seltenen Fällen beim Starten von PCMCIA das System stehen bleiben. Zu diesem Zeitpunkt ist die Installation aber schon weit genug fortgeschritten, so dass mit der Boot-Option NOPCMCIA=yes Linux ohne PCMCIA gestartet werden kann, zumindest im Textmodus. Hier hilft der Abschnitt *Wenn's trotzdem nicht geht* auf Seite 157 weiter. Evtl. kann man schon vor Abschluss des ersten Teils der Installation auf Konsole 2 einige Einstellungen am System verändern, so dass der Neustart erfolgreich verläuft.

Weitere Hilfsprogramme

Das Programm cardctl wurde schon mehrfach erwähnt. cardctl ist das wesentliche Werkzeug, um Informationen von PCMCIA zu erhalten, bzw. bestimmte Aktionen auszuführen. In der cardctl finden Sie Details; oder Sie geben cardctl ein und erhalten eine Liste der gültigen Kommandos.

Zu diesem Programm gibt es auch ein graphisches Frontend cardinfo (vgl. Abb. 8.1 auf der nächsten Seite), mit dem die wichtigsten Dinge kontrollierbar sind. Dazu muss jedoch das Paket pcmcia-cardinfo installiert sein.

Weitere Helfer aus dem pcmcia Paket sind ifport, ifuser, probe und rcpcmcia. Diese werden aber nicht immer benötigt. Um genau zu erfahren, was alles im Paket pcmicia steckt, verwendet man den Befehl rpm -ql pcmcia.

Kernel oder PCMCIA Paket aktualisieren

Wenn Sie den Kernel aktualisieren möchten, sollten Sie die von SuSE bereitgestellte Kernelpakete verwenden. Ist es notwendig, einen eigenen Kernel zu



Abbildung 8.1: *Das Programm cardinfo*

kompilieren, dann müssen auch die PCMCIA-Module neu kompiliert werden. Wichtig ist, dass während der Neuübersetzung bereits der richtige Kernel läuft, da aus diesem einige Informationen extrahiert werden. Das pcmcia Paket sollte bereits installiert, aber nicht gestartet sein; im Zweifelsfall also noch ein `rcpcmcia stop` ausführen. Dann installiert man das PCMCIA-Quellpaket mit und gibt anschließend ein:

```
rpm -ba /usr/src/packages/SPECS/pcmcia.spec
```

Danach liegen unter `/usr/src/packages/RPMS` neue Pakete. Das Paket `pcmcia-modules` enthält die PCMCIA Module für externes PCMCIA. Dieses Paket muss mit `rpm -force` installiert werden, da die Moduldateien offiziell zum Kernel-Paket gehören.

Weiterführende Informationen

Wer an Erfahrungen mit bestimmten Notebooks interessiert ist, sollte auf alle Fälle die Linux Laptop Homepage unter `http://linux-laptop.net` besuchen. Eine weitere gute Informationsquelle ist die Moblix-Homepage unter `http://mobilix.org/` (MobiliX – Mobile Computers and Unix). Dort findet man neben viele interessanten Informationen auch ein Laptop-Howto und ein IrDA-Howto. Außerdem gibt es in der Supportdatenbank den Artikel Laptops und Notebooks (PCMCIA) unter Linux `http://sdb.suse.de/de/sdb/html/laptop.html` (oder lokal unter `file:/usr/share/doc/sdb/de/html/laptop.html`).

SCPM – System Configuration Profile Management

Es gibt Situationen, in denen eine veränderte Konfiguration des Computersystems benötigt wird. Am häufigsten wird dies wohl auf mobile Computer zutreffen, die an verschiedenen Standorten betrieben werden. Es kann aber auch sein, dass man auf einem Desktopsystem zeitweilig andere Hardwarekomponenten verwendet. Oder aber man möchte einfach mal etwas ausprobieren. In jedem Fall sollte eine Rückkehr zum ursprünglichen System einfach sein. Noch besser ist es, wenn diese Umkonfiguration auch noch einfach reproduzierbar ist.

Eine Lösung für dieses Problem gab es bisher nur für PCMCIA Hardware. Dort konnte man verschiedene Konfigurationen in bestimmten Schemata ablegen. Ausgehend davon haben wir SCPM entwickelt, das die Beschränkung auf PCMCIA aufhebt. Mit dem „System Configuration Profile Management“ lässt sich ein frei wählbarer Teil der Systemkonfiguration festlegen, von dem verschiedene Zustände in eigenen Konfigurationsprofilen festgehalten werden können. Etwas freier ausgedrückt ist das, als ob man Schnappschüsse von seiner Systemkonfiguration macht, die man jederzeit wiederherstellen kann. Und der Bildausschnitt ist frei wählbar.

Das Hauptanwendungsgebiet wird vermutlich bei der Netzwerkkonfiguration von Laptops liegen. Aber bei unterschiedlichen Netzwerkeinstellungen verändern sich meist auch noch andere Elemente, z. B. die Einstellungen für E-Mail oder Proxies. Hierzu kommen unterschiedliche Drucker zuhause und in der Firma oder die gesonderte XFree86-Konfiguration für den Beamer bei Vorträgen, extra sparsame Stromverbrauchseinstellungen für unterwegs oder die andere Zeitzone in der Auslandsniederlassung.

Mit steigendem Einsatz dieses Werkzeugs werden immer wieder neue Anforderungen sichtbar. Wenn Sie selbst Anregungen und Kritik zu SCPM haben, dann nehmen Sie mit uns Kontakt auf. Wir sind sehr an Rückmeldungen interessiert. Wir haben versucht, SCPM auf ein flexibles Grundgerüst zu stellen, so dass z. B. auch ein serverbasiertes Profil Management möglich ist. Bitte teilen Sie uns Ihre Wünsche, Anregungen und Fehlerbeschreibungen über unser Webfrontend `http://www.suse.de/feedback` mit.

Grundbegriffe und Grundlagen

Vorab sollen einige Grundbegriffe festgelegt werden, die auch in der restlichen Dokumentation zu SCPM und im YaST2 Modul so verwendet werden.

- Unter *Systemkonfiguration* verstehen wir die gesamte Konfiguration des Computers. Alle grundlegenden Einstellungen, wie die z. B. Verwendung von Festplattenpartitionen oder Netzwerkeinstellungen, Zeitzonenauswahl oder Tastatureinstellung.

- Ein *Profil* oder auch *Konfigurationsprofil* ist ein Zustand der Systemkonfiguration, der festgehalten wurde und der bei Bedarf einfach wiederhergestellt werden kann.

- Als *aktives Profil* wird immer das Profil bezeichnet, in das zuletzt geschaltet wurde. Das heißt nicht, dass die aktuelle Systemkonfiguration exakt diesem Profil entspricht, denn die Konfiguration kann jederzeit individuell verändert werden.

- *Resource* im Sinne von SCPM sind alle Elemente, die zur Systemkonfiguration beitragen. Das kann eine Datei oder ein Softlink einschließlich ihrer Metadaten, wie Benutzer, Rechte, oder Zugriffszeit sein. Das kann aber auch ein Systemdienst sein, der einmal läuft und in einem anderen Profil ausgeschaltet ist.

- Für die häufigsten Anwendungsfälle gibt es vordefinierte *Resourcesets*. Durch die Auswahl eines solchen Resourcesets kann man einfach festlegen, welche Elemente der Systemkonfiguration von SCPM berücksichtigt werden. Bei Bedarf können auch eigene Resourcesets definiert werden. In der gegenwärtigen Entwicklungsstufe von SCPM verwenden alle Profile dasselbe Set. Eine Weiterentwicklung hin zu Profilen, die unterschiedliche Ressourcen behandeln, ist jedoch bereits bedacht.

SCPM YaST2 Modul und weiterführende Dokumentation

Als grafisches Frontend zu SCPM gibt es ein YaST2 Modul als Alternative zu dem Kommandozeilen-Frontend. Da die Funktionalität beider Frontends im wesentlichen dieselbe ist und die Kenntnis des Kommandozeilen-Frontends für viele Zwecke interessant ist, wird hier nur das letztere beschrieben. Die Bedienung des SCPM YaST2 Moduls ist danach zusammen mit den dort angebotenen Hilfetexten sehr leicht. Die wenigen Besonderheiten des YaST2 Moduls werden an passender Stelle erwähnt.

Die aktuellste Dokumentation wird immer in den Infoseiten zu SCPM zu finden sein. Diese kann mit Werkzeugen wie Konqueror oder Emacs eingesehen werden (`konqueror info:scpm`). In der Konsole verwendet man `info` oder `pinfo`. Technische Dokumentation für Leute, die selbst Hand an SCPM legen möchten, gibt es unter `/usr/share/doc/packages/scpm`.

Der Aufruf von `scpm` ohne weitere Argumente gibt eine Kommandoübersicht aus.

SCPM einrichten

Bevor mit SCPM gearbeitet werden kann, muss es erst einmal eingeschaltet werden. Es ist jedoch sehr empfehlenswert, zuerst ein Resourceset aus `/lib/scpm/resource_sets/` auszuwählen. Das ausgewählte Set wird in `/etc/scpm.conf` in die Variable ⟨*RESOURCE_SET*⟩ eingetragen. Wird kein Resourceset eingetragen, versucht SCPM aus verschiedenen Informationsquellen eine sinnvolle Menge von behandelten Ressourcen zusammenzustellen. Diese ist jedoch für viele Anwendungsfälle zu umfangreich.

Um seinen eigenen Anforderungen am besten gerecht zu werden, können unter `/var/lib/scpm/resource_sets` eigene Resourcesets angelegt werden. Es gilt dabei keineswegs der Grundsatz „Viel hilft viel". Jede Änderung, die für alle Profile gelten soll, an einer Datei, die von SCPM behandelt wird, muss dann sooft durchgeführt werden, wie es Profile gibt. Deshalb ist die gesamte Konfiguration aller Profile um so komplexer, je größer ein Resourceset ist. Die Wahl des Resourcesets kann jederzeit geändert werden, wobei jedoch nur der Wechsel von kleineren Sets zu größeren immer problemlos ist. Beim Verkleinern des verwendeten Resourcesets muss nämlich immer bedacht werden, welche Version einer Resource (aus welchem Profil) behalten und welche verworfen wird.

Mit dem Aufruf von `scpm enable` wird SCPM eingeschaltet. Beim ersten Einschalten wird SCPM initialisiert, was einige Sekunden in Anspruch nimmt. SCPM kann mit `scpm disable` jederzeit ausgeschaltet werden, um unbeabsichtigte Profilumschaltungen zu vermeiden. Beim anschließenden Wiedereinschalten wird die Initialisierung einfach fortgesetzt.

Profile anlegen und verwalten

Nachdem SCPM eingeschaltet wurde, gibt es bereits ein Profil namens `default`. Eine Liste aller verfügbaren Profile gibt das Kommando `scpm list` aus. Dieses bisher einzige Profil ist zwangsläufig auch das aktive Profile. Das erfährt man mit `scpm active`. Das Profil `default` ist als Grundkonfiguration gedacht, von der die anderen Profile abgeleitet werden. Deshalb sollten zuerst alle Einstellungen, die in allen Profilen einheitlich sein sollen, vorgenommen werden. Mit `scpm reload` werden diese Änderungen dann im aktiven Profil gespeichert. Das Profil `default` kann dennoch beliebig verwendet, umbenannt oder gelöscht werden.

Es gibt zwei Möglichkeiten, ein neues Profil hinzuzufügen. Wenn das neue Profil (hier mit Namen `work`) z. B. auf dem Profil `default` basieren soll, geschieht dies mit `scpm copy default work`. Danach kann man mit `scpm switch work` in das neue Profil umschalten und es dann konfigurieren. Manchmal hat man aber auch die Systemkonfiguration schon für bestimmte Zwecke verändert und möchte diese danach in einem neuen Profil festhalten. Das erledigt der Aufruf von `scpm add work`. Jetzt ist die aktuelle Systemkonfiguration im Profil `work` gesichert und das neue Profil als aktiv markiert; d. h. ein `scpm reload` sichert Änderungen jetzt im Profil `work`.

Selbstverständlich können Profile auch umbenannt oder gelöscht werden. Dafür gibt es die Kommandos `scpm rename x y` und `scpm delete x`. Um z. B. `work` nach `arbeit` umzubenennen und es hinterher zu löschen, gibt man `scpm rename work arbeit` und dann `scpm delete arbeit` ein. Nur das aktive Profil kann nicht gelöscht werden.

Nochmal die einzelnen Kommandos:

`scpm list` gibt alle verfügbaren Profile aus

`scpm active` gibt das aktive Profile aus

`scpm add ⟨name⟩` speichert die gegenwärtige Systemkonfiguration in einem neuen Profil und macht dieses zum aktiven

`scpm copy ⟨quellname⟩ ⟨zielname⟩` kopiert ein Profil

`scpm rename ⟨quellname⟩ ⟨zielname⟩` benennt ein Profil um

`scpm delete ⟨name⟩` löscht ein Profil

Hinweis zum YaST2 Modul: Hier gibt es nur den Knopf 'Add'. Es erscheint dann aber die Frage, ob man ein existierendes Profil kopieren oder die gegenwärtige Systemkonfiguration Systemkonfiguration sichern möchte. Zum Umbenennen verwende man dort den Knopf 'Edit'.

Zwischen Konfigurationsprofilen umschalten

Das Umschalten zu einem anderen Profil (hier `work`) wird mit dem Kommando `scpm switch work` ausgelöst. Es ist zulässig, zum gerade aktiven Profile umzuschalten um geänderte Einstellungen an der Systemkonfiguration zu sichern. Alternativ kann dafür aber auch das Kommando `scpm reload` verwendet werden.

Um den Umschaltvorgang und die dabei evtl. auftretenden Fragen besser zu verstehen, soll dieser hier näher erläutert werden.

Zuerst prüft SCPM, welche Ressourcen des aktiven Profils seit dem letzten Umschalten verändert wurden. Für alle veränderten Ressourcen wird dann nachgefragt, ob die Änderung an dieser Resource in das immer noch aktive Profil übernommen oder verworfen werden soll. Diese Fragen betreffen insofern nur das Profil, das man gerade verlassen möchte.

Danach vergleicht SCPM die aktuelle Systemkonfiguration mit dem neuen Profil, in das umgeschaltet werden soll. Dabei wird ermittelt, welche Systemdienste aufgrund von Konfigurationsänderungen oder wegen gegenseitiger Abhängigkeiten angehalten bzw. (wieder) gestartet werden müssen. Das kann man sich wie einen teilweisen Systemreboot vorstellen, nur dass eben nur ein kleiner Teil des Systems betroffen ist und der Rest unverändert weiterarbeitet.

Erst jetzt werden die

1. Systemdienste angehalten,
2. alle veränderten Ressourcen (i. a. Konfigurationsdateien) geschrieben und die
3. Systemdienste (wieder) gestartet.

Erweiterte Profileinstellungen

Sie können für jedes Profil eine Beschreibung eingeben, die dann bei `scpm list` mit ausgegeben wird. Eingeben kann man diese Beschreibung für das gerade aktive Profil mit dem Kommando `scpm set description "text"`. Für nicht aktive Profile muss noch das Profil angegeben werden, also `scpm set description "text"work`. Manchmal kommt es vor, dass beim Umschalten in ein anderes Profil zusätzliche Aktionen ausgeführt werden sollen, die in SCPM (noch) nicht vorgesehen sind. Dafür können für jedes Profil vier ausführbare Programme oder Scripte eingehängt werden, die zu verschiedenen Zeitpunkten während das Umschaltens ausgeführt werden. Diese Zeitpunkte sind:

prestop vor dem Anhalten von Diensten beim Verlassen des Profils

poststop nach dem Anhalten von Diensten beim Verlassen des Profils

prestart vor dem Starten von Diensten beim Aktivieren des Profils

poststart nach dem Starten von Diensten beim Aktivieren des Profils

Das Umschalten von Profil `work` zu Profil `home` läuft dann folgendermaßen ab:

1. Prestop-Aktion des Profils `work` wird ausgeführt.
2. Anhalten von Diensten
3. Poststop-Aktion des Profils `work` wird ausgeführt
4. Verändern der Systemkonfiguration
5. Prestart-Aktion des Profils `home` wird ausgeführt.
6. Starten von Diensten
7. Poststart-Aktion des Profils `home` wird ausgeführt.

Diese Aktionen werden auch mit dem `set` Kommando eingehängt, nämlich mit `scpm set prestop` ⟨*dateiname*⟩, `scpm set poststop` ⟨*dateiname*⟩, `scpm set prestart` ⟨*dateiname*⟩ oder `scpm set poststart` ⟨*dateiname*⟩. Es muss sich dabei um ein ausführbares Programm handeln, d. h. Scripte müssen den richtigen Interpreter beinhalten und zumindest für den Superuser ausführbar sein.

Alle Zusatzeinstellungen, die mit `set` eingegeben wurden, lassen sich mit `get` abfragen. Zum Beispiel liefert `scpm get poststart` den Namen des Poststartprogramms oder einfach keine Information, wenn nichts eingehängt wurde. Gelöscht werden solche Einstellungen durch Überschreiben mit `""`; d. h. ein `scpm set prestop` "" hängt das Poststop-Programm wieder aus.

Genau wie beim Anlegen der Beschreibung können alle `set` und `get` Kommandos für ein beliebiges Profil angewandt werden. Dazu wird zuletzt noch der Name des Profils angegeben. Zum Beispiel `scpm get prestop` ⟨*dateiname*⟩ `work` oder `scpm get prestop work`.

Achtung

Da diese Skripte oder Programme mit den Rechten des Superusers ausgeführt werden sollten sie nicht von beliebigen Anwendern änderbar sein. Da in Scripten durchaus vertrauliche Informationen enthalten sein können, ist es sogar angeraten, dass diese nur vom Superuser lesbar sind. Am besten versieht man diese Programme mit den Rechten `-rwx---- root root`.
(`chmod 700` ⟨*dateiname*⟩ und `chown root.root` ⟨*dateiname*⟩)

Achtung

Profilauswahl beim Booten

Es ist möglich, schon vor dem Booten ein Profil auszuwählen. Dazu muss lediglich der Bootparameter `PROFILE=`⟨*Name des Profils*⟩ am Bootprompt eingegeben werden.

Bei der Option `title` verwendet man dann ebenfalls den Namen des Profils. Standardmäßig wird GRUB als Bootloader verwendet. Eine ausführlichere Beschreibung finden Sie Abschnitt *Booten mit GRUB* auf Seite 107; alternativ geben Sie `info grub` ein. Die Konfiguration von GRUB sieht dann z. B. wie folgt aus:

```
gfxmenu (hd0,5)/boot/message
color white/green black/light-gray
default 0
timeout 8

title work
   kernel (hd0,5)/boot/vmlinuz-2.4.19-4GB root=/dev/hda6 PROFILE=work
   initrd (hd0,5)/boot/initrd-2.4.19-4GB

title home
   kernel (hd0,5)/boot/vmlinuz-2.4.19-4GB root=/dev/hda6 PROFILE=home
   initrd (hd0,5)/boot/initrd-2.4.19-4GB

title road
   kernel (hd0,5)/boot/vmlinuz-2.4.19-4GB root=/dev/hda6 PROFILE=road
   initrd (hd0,5)/boot/initrd-2.4.19-4GB
```

Datei 9: *Die Datei /boot/grub/menu.lst*

Für Systeme, die noch den Bootloader LILO verwenden, kann die Datei 10 verwendet werden.

```
boot    = /dev/hda
change-rules
reset
read-only
menu-scheme = Wg:kw:Wg:Wg
prompt
timeout = 80
message = /boot/message
```

```
image  = /boot/vmlinuz
label  = home
root   = /dev/hda6
initrd = /boot/initrd
append = "vga=0x317 hde=ide-scsi PROFILE=home"

image  = /boot/vmlinuz
label  = work
root   = /dev/hda6
initrd = /boot/initrd
append = "vga=0x317 hde=ide-scsi PROFILE=work"

image  = /boot/vmlinuz
label  = road
root   = /dev/hda6
initrd = /boot/initrd
append = "vga=0x317 hde=ide-scsi PROFILE=road"
```

Datei 10: *Datei /etc/lilo.conf*

Jetzt kann beim Booten sehr einfach das gewünschte Profil ausgewählt werden.

APM und ACPI – Powermanagement

Powermanagement setzt eine dafür ausgelegte Hardware und passende BIOS-Routinen voraus. Die meisten Notebooks und viele moderne Desktops bringen diese Voraussetzungen mit. Bisher wurde dazu meist der APM Standard verwendet (engl. *Advanced Power Management*). Dies sind im wesentlichen Funktionen, die im BIOS des Computers implementiert sind. Deshalb funktioniert Powermanagement nicht auf allen Geräten gleich gut. Wenn Sie ein Notebook mit funktionierender APM Implementierung haben, dann tun Sie gegenwärtig gut daran, diese zu verwenden. Es gibt nämlich seit einiger Zeit Hersteller, die sich APM sparen und vollständig auf den neueren Standard ACPI (engl. *Advanced Configuration and Power Interface*) setzen. ACPI ist aber schon konzeptionell schwieriger und setzt gute Zusammenarbeit von Hardwareherstellern, BIOS-Programmieren und den Betriebssystemexperten voraus. Außerdem ist die ACPI Implementierung im Linux Kernel ist noch nicht fertig und deswegen nur teilweise nutzbar. Erst mit dem Kernel 2.6 ist hier eine wesentliche Besserung in Sicht.

Stromsparfunktionen

Viele dieser Funktionen sind von allgemeinem Interesse, aber so richtig wichtig sind diese aber erst im mobilen Einsatz. Im Folgenden werden diese Funktionen beschrieben und erklärt von welchem System diese ausgeführt werden können.

Stand-by In dieser Betriebsart wird nur das Display ausgeschaltet und bei manchen Geräten die Prozessorleistung gedrosselt. Nicht jedes APM stellt diese Funktion zur Verfügung. Bei ACPI entspricht das dem Zustand S2.

Suspend (to memory) Hier wird der gesamte Systemzustand in den Arbeitsspeicher geschrieben und außer diesem das gesamte System schlafen gelegt. In diesem Zustand braucht der Computer nur sehr wenig Strom, sodass man damit je nach Gerät von 12 Stunden bis mehrere Tage mit Batterie überbrücken kann. Der Vorteil dieses Zustands ist, dass man innerhalb weniger Sekunden wieder an derselben Stelle weiterarbeiten kann, ohne erst booten und benötigte Programme neu laden zu müssen. Bei den meisten modernen Geräten genügt es, den Deckel zu schließen, um zu suspendieren, und ihn zum Weiterarbeiten einfach wieder zu öffnen und es kann sofort weitergehen. Bei ACPI entspricht das dem Zustand S3.

Hibernation (Suspend to disk) In dieser Betriebsart hält es der Computer länger als einen Winter aus (Hibernation bedeutet Überwinterung), denn der Systemzustand wird vollständig auf der Festplatte gespeichert und das System danach ausgeschaltet. Die Rückkehr aus dem Winterschlaf dauert zwischen 30 - 90 Sekunden und auch hier wird der Zustand vor dem Suspend genau wiederhergestellt. Einige Hersteller bieten in ihrem APM sinnvolle Mischformen davon an (z. B. RediSafe bei IBM Thinkpads). Hibernation entspricht bei ACPI dem Zustand S4. Es gibt für Linux auch eine reine Softwarelösung, die in SuSE Linux aber nicht enthalten ist. Wer dies Verwenden möchte muß selbst die Ärmel hochkrempeln: `http://falcon.sch.bme.hu/~seasons/linux/swsusp.html`

Kontrolle des Akkuzustands Neben der reinen Information über den Ladezustand, ist es auch wichtig, daß etwas unternommen wird, wenn die Energiereserven knapp werden. Auch das wird meist von den APM BIOSroutinen erledigt. Alternativ kann dazu auch der `apmd/acpid` oder `klaptopdaemon` verwendet werden.

Automatisches Ausschalten Nach einem Shutdown wird der Computer vollständig ausgeschaltet. Das ist vor allem von Bedeutung, wenn ein automatischer Shutdown ausgeführt wird, kurz bevor der Akku leer ist.

Abschalten von Systemkomponenten Die wesentliche Komponente um Energie zu sparen ist die Festplatte. Je nach Zuverlässigkeit des gesamten Systems kann diese mehr oder weniger lang schlafen gelegt werden. Allerdings steigt das Risiko eines Datenverlusts mit der Länge der Ruhepausen der Platte. Andere Komponenten können via ACPI/footnotezumindest theoretisch oder dauerhaft im BIOSsetup deaktiviert werden. Vor allem der Infrarotport sollte möglichst ausgeschaltet bleiben, solange man diesen nicht benötigt (siehe xxxIRDAxxx).

Kontrolle der Prozessorleistung Zusammen mit APM gibt es meist nur die Möglichkeit im BIOSsetup verschiedene Einstellungen zu wählen. Kontrollieren läßt sich die Prozessorfrequenz mit dem Programm `procspeed` aus dem Paket `apmd`.

APM

Einige der Stromsparfunktionen führt das APM-BIOS alleine aus. Stand-by und Suspend kann man auf vielen Notebooks mit Tastenkombinationen oder mit Schließen des Deckels aktivieren. Dazu ist erstmal keinerlei Funktion seitens des Betriebssystems nötig. Wer diese Betriebsarten jedoch per Kommando einleiten möchte, darauf angewiesen ist, dass vor dem Suspend noch bestimmte Aktionen ausgeführt werden, oder einfach nur den Ladezustand der Batterie angezeigt bekommen möchte, muss entsprechende Pakete und einen geeigneten Kernel installiert haben.

Bei den fertigen Kerneln von SuSE Linux ist der APM Support fest eingebaut und wird automatisch aktiviert, sobald beim Booten ein APM-BIOS gefunden wird. Um den APM Support auszuschalten kann am Bootprompt `apm=off` verwendet werden. Ob APM aktiviert wurde lässt sich leicht mit dem Kommando `cat /proc/apm` nachprüfen. Wenn hier eine Zeile mit diversen Zahlen erscheint, ist alles okay. Jetzt sollte ein `shutdown -h` zum Ausschalten des Computers führen.

Da manche BIOS-Implementierungen sich nicht exakt an Standards halten, kommt es manchmal zu merkwürdigem Verhalten. Manche Probleme kann man mit speziellen Bootparametern umgehen (früher waren dies Kernelkonfigurationsoptionen). Alle Parameter werden am Bootprompt in der Form `apm=`⟨*parameter*⟩ eingegeben:

on/off APM Support ein/ausschalten

(no-)allow-ints Während dem Ausführen von BIOS Funktionen Interrupts zulassen

(no-)broken-psr BIOS hat eine kaputte „GetPowerStatus“ Funktion

(no-)realmode-power-off Den Prozessor vor dem Shutdown in den Real Mode zurückschalten

(no-)debug APM Ereignisse im Syslog protokollieren

(no-)power-off Nach dem Shutdown das System ausschalten

bounce-interval=⟨*n*⟩ Zeit in 1/100 Sekunden, in der nach einem Suspendereigniss weitere Suspendereignisse ignoriert werden

idle-threshold=⟨*n*⟩ Prozentsatz der Systeminaktivität, ab der die BIOS Funktion idle aufgerufen wird (0=immer, 100=nie)

idle-period=⟨*n*⟩ Zeit in 1/100 Sekunden, über der die System(in)aktivität ermittelt wird

Der APM-Daemon (apmd)

Der Daemon `apmd` dient zur Überwachung der Batterie und kann bestimmte Aktionen auslösen, wenn ein Stand-by oder Suspend Ereignis eintritt. Er befindet sich im Paket apmd. Er ist nicht unbedingt zum Betrieb notwendig, kann jedoch bei manchen Problemen recht nützlich sein.

Der apmd wird nicht automatisch beim Booten gestartet. Ist dies jedoch erforderlich, kann man mit dem YaST2 Runlevel-Modul die Einstellungen zu den Systemdiensten verändern. Alternativ kann auch das Programm `chkconfig` verwendet werden. Siehe Abschnitt *Runlevel-Editor* auf Seite 84. Manuell kann er mit dem Kommando `rcapmd start` gestartet werden.

Zur Konfiguration gibt es in `/etc/sysconfig/powermanagement` einige Variablen. Die Datei ist mit Kommentaren versehen, deshalb werden hier nur einige Hinweise gegeben.

APMD_ADJUST_DISK_PERF Damit wird veranlasst, daß das Verhalten der Festplatte an den Zustand der Stromversorgung angepasst wird. Dazu gibt es eine Reihe weiterer Variablen, die entweder mit `APMD_BATTERY` oder `APMD_AC` beginnen. Die ersteren enthalten die Einstellungen für den Batteriebterieb, die letzteren die für den Betrieb mit externer Stromversorgung.

APMD_BATTERY/AC_DISK_TIMEOUT Nach welcher Zeit Platteninaktivität wird diese angehalten. Die möglichen Werte sind im Abschnitt *Pause für die Festplatte* auf Seite 177 oder in der Manpage zu `hdparm` Option `-S` beschrieben.

APMD_BATTERY/AC_KUPDATED_INTERVAL Die Zeit zwischen zwei Läufen des Kernel Update Deamons.

APMD_BATTERY/AC_DATA_TIMEOUT Das maximale Alter gepufferter Daten.

APMD_BATTERY/AC_FILL_LEVEL Der maximale Füllstand des Festplattenpuffers.

APMD_PCMCIA_EJECT_ON_SUSPEND Obwohl PCMCIA bei mit APM-Unterstützung übersetzt ist, gibt es hier manchmal Schwierigkeiten. Einige der Kartentreiber kehren von einem Suspend nicht ordentlich zurück (`xirc2ps_cs`). Deshalb kann der apmd das PCMCIA-System vor dem Suspend deaktivieren und danach wieder aktivieren. Dazu wird die Variable `APMD_PCMCIA_EJECT_ON_SUSPEND` auf `yes` gesetzt.

APMD_INTERFACES_TO_STOP Hier können Netzwerkinterfaces eingetragen werden, die vor dem Suspendieren angehalten und danach wieder gestartet werden sollen.

APMD_INTERFACES_TO_UNLOAD Wenn außerdem noch die Teribermodule dieser Interfaces entladen werden müssen, ist diese Variable zu verwenden.

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND Machmal kommt es auch vor, daß das Wiederaufwachen nach einem Suspend nicht funktioniert, wenn ein IDE Gerät (Festplatte) noch im DMA Modus ist.

Es gibt noch weitere Möglichkeiten, wie z. B. Tastaturwiederholrate oder die Uhrzeit nach einem Suspend zu korrigieren oder den Laptop automatisch herunterzufahren, wenn die das APM-BIOS ein „Batterie kritisch"-Ereignis sendet. Wer noch speziellere Aktionen ausführen möchte, der kann das Script `/usr/sbin/apmd_proxy`, das die oben aufgeführten Jobs ausführt, an seine Bedürfnisse anpassen.

Weitere Befehle

Im apmd sind noch einige nützliche Programme enthalten. Mit apm kann die aktuelle Batteriekapazität abgefragt werden und das System in Stand-by

(apm -S) oder Suspend (apm -s) geschickt werden; vgl. die Manual-Page von apm (man apm).

Das Kommando apmsleep suspendiert das System für eine vorgegebene Zeit; vgl. apmsleep.

Wer eine Logdatei beobachten möchte, ohne die Festplatte ständig am Laufen zu halten, der kann tailf als Ersatz für tail -f verwenden.

Natürlich gibt es auch hier Tools für das X Window System. Ebenfalls im apmd findet man xapm, was den Ladezustand der Batterie grafisch anzeigt. Wer den KDE-Desktop verwendet – oder zumindest kpanel –, kann sich auch von kbatmon den Ladestand des Akkus anzeigen lassen und das System suspendieren. Als Alternative ist auch xosview interessant.

ACPI

Um ACPI verwenden zu können, darf APM nicht aktiviert werden. Wenn der Kernel kein APM-BIOS erkennt, geschieht dies automatisch. Ansonsten kann am Bootprompt der Parameter apm=off verwendet werden. Natürlich muß der Computer ACPI 2.0 oder neuer unterstützen. Ob ACPI aktiviert wurde, kann in den Bootmeldungen des Kernels in /var/log/boot.msg nachgesehen werden.

Danach müssen jedoch noch eine Reihe von Modulen für das OSPM (Operating System Power Management) geladen werden. Diese werden vom Startscript des ACPI-Daemons geladen. Wenn eines dieser Module Probleme bereitet, kann es in /etc/sysconfig/powermanagement vom Laden ausgeschlossen werden.

Jetzt findet man unter /proc/acpi eine Reihe von Dateien, die über den Systemzustand informieren oder über die Aktionen wie Suspend ausgelöst werden können. Allerdings funktioniert hier noch längst nicht alles, weil es sich noch in der Entwicklung befindet. Was funktioniert und was nicht, ist jedoch auch stark vom verwendeten Computer abhängig. Hier hilft nur ausprobieren.

Der ACPI-Daemon (acpid)

Ähnlich wie der APM Daemon verarbeitet der ACPI Daemon bestimmte ACPI Ereignisse. Diese sind zur Zeit lediglich die Ereignisse, daß bestimmte Schalter, wie der Ein/Aus-Schalter oder der Deckelkontakt, betätigt wurden. Alle Ereignisse werden im Systemlog protokolliert. In /etc/sysconfig/powermanagement kann in den Variablen ACPI_BUTTON_POWER und ACPI_BUTTON_LID festgelegt werden, was bei diesen Ereignissen geschehen

soll. Wem das nicht genügt, der kann das Script /usr/sbin/acpid_proxy anpassen oder die Konfiguration des acpid unter /etc/acpi/ verändern.

Pause für die Festplatte

Man kann unter Linux die Festplatte abschalten, wenn sie nicht benötigt wird. Dazu dient das Programm hdparm, mit dem man diverse Einstellungen an den Festplatten vornehmen kann. Mit der Option -y wird die Platte sofort in den Stand-by-Modus geschickt, mit -Y (Vorsicht!) wird sie vollständig abgeschaltet. Mit hdparm -S ⟨x⟩ wird erreicht, dass die Platte nach einer bestimmten Zeit Inaktivität abgeschaltet wird. Der Platzhalter ⟨x⟩ hat leicht unterschiedliche Bedeutung: 0 schaltet diesen Machanismus aus, die Platte läuft immer. Werte von 1 bis 240 werden mit 5 Sekunden multipliziert. 241 bis 251 entsprechen 1 bis 11 mal 30 Minuten.

Häufig ist es aber nicht ganz so einfach, denn es gibt unter Linux eine Vielzahl von Prozessen, die Daten auf die Platte schreiben und dadurch die Platte wieder aufwecken. Deshalb ist es an dieser Stelle wichtig zu verstehen wie Linux mit Daten umgeht, die auf die Platte geschrieben werden sollen.

Alle Daten werden zuerst in einen Puffer im Arbeitsspeicher geschrieben. Dieser Puffer wird vom „Kernel Update Daemon“ (kupdated) überwacht. Immer wenn Daten ein bestimmtes Alter erreichen oder wenn der Puffer bis zu einem gewissen Grad gefüllt ist, wird der Puffer geleert und die Daten der Festplatte übergeben. Die Größe des Puffers ist übrigens dynamisch und hängt von der Speichergröße und der Systemauslastung ab. Da das vorrangige Ziel Datensicherheit ist, ist der kupdated standardmäßig auf kleine Zeitintervalle eingestellt. Er prüft den Puffer alle 5 Sekunden und benachrichtigt bdflush-Daemon, wenn Daten älter als 30 Sekunden sind oder der Puffer zu 30% gefüllt ist. Der bdflush-Daemon schreibt dann die Daten uf die Platte. Er schreibt auch unabhängig vom kupdated wenn z. B. der Puffer voll ist. Wer ein stabiles System hat kann diese Einstellungen nun verändern. Man muß sich jedoch immer darüber im klaren sein, daß dies auf Kosten der Datensicherheit geht.

Die Einstellungen findet man mit cat /proc/sys/vm/bdflush. Der erste Wert ist der Füllgrad des Puffers ab dem der Puffer geleert wird. Der sechste Wert ist das maximale Alter von Daten im Puffer in 1/100 Sekunden. Der fünfte Wert ist das Interval in dem kupdated den Puffer prüft auch in 1/100 Sekunden. Um z. B. das kupdated-Interval auf 1 Minute zu vergrößern schreibt man neue Zahlen in diese Datei mit

```
echo 30 500 0 0 6000 > /proc/sys/vm/bdflush
```

Die Werte vor dem zu verändernden Wert werden dabei einfach abgeschrie-

ben, die Werte danach kann man weglassen. So ändert

```
echo 60 > /proc/sys/vm/bdflush
```

den auslösenden Füllgrad des Puffers auf 60%. Die restlichen Werte sind in den Kernelquellen in der Datei `Documentation/filesystems/proc.txt` beschrieben.

Vorsicht: Änderungen an den Einstellungen des Kernel Update Daemon beeinflussen die Datensicherheit. Wer sich unsicher ist, läßt lieber die Finger davon.

Die Einstellungen für den Festplattentimeout, den kupdated-Interval, den Füllgrad des Puffers und das Alter der Daten können in `/etc/sysconfig/powermanagement` zweifach abgelegt werden: einmal für den Batteriebetrieb und einmal für den Betrieb mit externer Stromversorgung. Die Variablen sind im Abschnitt über den apmd und in der Datei selbst beschrieben.

Neben all diesen Vorgängen schreiben sogenannte „Journaling Dateisysteme“ wie z. B. ReiserFS oder Ext3 unabhängig von `bdflush` ihre Metadaten auf die Festplatte, was natürlich auch ein Einschlafen der Platte verhindert. Zur Zeit der Dokumentationserstellung, respektieren Ext3/JBD den 5. Wert in `/proc/sys/vm/bdflush` und schreiben dann auch seltener ihre Metadaten, wenn dieser Wert erhöht wurde. Für ReiserFS wird das gerade implementiert. Voraussichtlich soll also auch dieses Filesystem ein Suspendieren nicht mehr verhindern. Im Zweifelsfall ist es das beste, auf das gute alte Ext2-Dateisystem zurückzugreifen.

Weiterhin ist natürlich zu beachten, wie sich die Programme verhalten, die man gerade verwendet. Zum Beispiel schreiben gute Texteditoren regelmäßig versteckte Sicherungen der gerade geänderten Datei auf die Platte. Das weckt dann die Platte immer wieder auf. Solche Eigenschaften von Programmen können auch abgeschaltet werden, aber auch hier wieder auf Kosten der Datensicherheit.

In diesem Zusammenhang gibt es für den Maildaemon `postfix` eine Variable `POSTFIX_LAPTOP`. Wenn diese auf `yes` gesetzt wird greift postfix wesentlich seltener auf die Festplatte zu. Das ist jedoch nicht von Bedeutung, wenn das Intervall für den `kupdated` verlängert wurde.

IrDA – Infrared Data Association

IrDA („Infrared Data Association“) ist ein Industriestandard für drahtlose Kommunikation über Infrarotlicht. Viele heute ausgelieferte Laptops sind mit

einem IrDA-kompatiblen Sender/Empfänger ausgestattet, der die Kommunikation mit anderen Geräten wie Druckern, Modems, LAN oder anderen Laptops ermöglicht. Die Übertragungsrate reicht von 2400 bps bis hin zu 4 Mbps.

Es gibt zwei Betriebsmodi für IrDA. Im Standardmodus SIR wird der Infrarotport über eine serielle Schnittstelle angesprochen. Dieser Modus funktioniert auf fast allen Geräten und genügt für viele Anforderungen. Der schnellere Modus FIR benötigt einen speziellen Treiber für den IrDA Chip. Es gibt aber nicht für alle Chips solche Treiber. Außerdem muss der gewünschte Modus im BIOS Setup des Computers eingestellt werden. Dort erfährt man meist auch, welche serielle Schnittstelle für den SIR Modus verwendet wird.

Informationen zu IrDA finden Sie im IrDA-Howto von Werner Heuser unter `http://mobilix.org/Infrared-HOWTO/Infrared-HOWTO.html` und auf der Homepage des Linux IrDA Projekts `http://irda.sourceforge.net/`.

Software

Die notwendigen Kernelmodule sind im Kernelpaket enthalten. Das Paket `irda` stellt die nötigen Hilfsprogramme zur Unterstützung der Infrarotschnittstelle bereit. Nach der Installation des Paketes findet man die Dokumentation unter `/usr/share/doc/packages/irda/README`.

Konfiguration

Der IrDA Systemdienst wird nicht automatisch beim Booten gestartet. Verwenden Sie das YaST2 Runlevel-Modul um die Einstellungen zu den Systemdiensten zu verändern. Alternativ kann auch das Programm `chkconfig` verwendet werden. Siehe auch Abschnitt *Runlevel-Editor* auf Seite 84. Leider benötigt IrDA merklich mehr (Batterie-)Strom, da alle paar Sekunden ein Discovery-Paket verschickt wird, um andere Peripheriegeräte automatisch zu erkennen. Deshalb sollte man, wenn man auf Batteriestrom angewiesen ist, IrDA am besten nur bei Bedarf starten, Mit dem Kommando

```
rcirda start
```

können Sie die Schnittstelle jederzeit manuell aktivieren bzw. deaktivieren (mit dem Parameter `stop`). Beim Aktivieren der Schnittstelle werden die notwendigen Kernel-Module automatisch geladen.

In der Datei `/etc/sysconfig/irda` gibt es nur eine Variable ⟨*IRDA_PORT*⟩. Dort können Sie einstellen welche Schnittstelle im SIR Modus verwendet wird; dies wird über das Skript `/etc/irda/drivers` beim Start der Infrarotunterstützung eingestellt.

Verwendung

Will man nun über Infrarot drucken, kann man dazu über die Gerätedatei `/dev/irlpt0` die Daten schicken. Die Gerätedatei `/dev/irlpt0` verhält sich wie die normale drahtgebundene Schnittstelle `/dev/lp0`, nur dass die Druckdaten drahtlos über infrarotes Licht verschickt werden.

Einen Drucker, der über die Infrarotschnittstelle betrieben wird, können Sie wie einen Drucker am Parallelport oder an der seriellen Schnittstelle über einrichten. Beachten Sie bitte beim Drucken, dass sich der Drucker in Sichtweite der Infrarotschnittstelle des Computers befindet und dass die Infrarotunterstützung gestartet wird.

Will man über die Infrarotschnittstelle mit anderen Rechnern, mit Handys oder ähnlichen Geräten kommunizieren, so kann man dies über die Gerätedatei `/dev/ircomm0` erledigen. Mit dem Siemens S25 Handy beispielsweise kann man sich über das Programm wvdial mittels Infrarot drahtlos ins Internet einwählen. Auch ein Datenabgleich mit dem Palm Pilot ist so möglich, dazu muss im entsprechenden Programm als Gerät einfach `/dev/ircomm0` eingegeben werden.

Beachten Sie bitte auch, dass Sie ohne weiteres nur Geräte ansprechen können, die die Protokolle Printer oder IrCOMM unterstützen. Mit speziellen Programmen (`irobexpalm3`, `irobexreceive`, bitte beachten Sie hierzu die Beschreibung im IR-HOWTO) können Sie auch Geräte ansprechen, die das IROBEX-Protokoll verwenden (3Com Palm Pilot). Die vom Gerät unterstützten Protokolle werden bei der Ausgabe von irdadump nach dem Gerätenamen in eckigen Klammern angeben. Die Unterstützung des IrLAN-Protokolls ist „work in progress“ – es ist leider zur Zeit noch nicht stabil, wird aber sicher in naher Zukunft auch unter Linux zur Verfügung stehen.

Troubleshooting

Falls Geräte am Infrarotport nicht reagieren, können Sie als Benutzer root mit dem Kommando irdadump überprüfen, ob das andere Gerät vom Computer erkannt wird:

```
irdadump
```

Bei einem Canon BJC-80 Drucker in Sichtweite des Computers erscheint dann eine Ausgabe ähnlich der folgenden in regelmäßiger Wiederholung (vgl. Ausgabe 4.

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [ Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* erde
                        hint=0500 [ PnP Computer ] (21)
```

Ausgabe 4: *IrDA: irdadump*

Sollte überhaupt keine Ausgabe erfolgen oder das andere Gerät sich nicht zurückmelden, so überprüfen Sie bitte die Konfiguration der Schnittstelle. Verwenden Sie überhaupt die richtige Schnittstelle? Manchmal ist die Infrarotschnittstelle auch unter `/dev/ttyS2` oder `/dev/ttyS3` zu finden oder ein anderer Interrupt als Interrupt 3 wird verwendet. Diese Einstellungen können Sie aber bei fast jedem Laptop im BIOS-Setup konfigurieren.

Mit einer einfachen Video-Kamera können Sie auch überprüfen, ob die Infrarot-LED überhaupt aufleuchtet – im Gegensatz zum menschlichen Auge können die meisten Videokameras Infrarotlicht sehen.

Teil III

System

Der Linux Kernel

Der Kernel ist das Innerste des Linux Systems. Auf den folgenden Seiten wird man nicht lernen, wie man Kernel-„Hacker“ wird, aber man erfährt, wie man ein Kernel-Update durchführt, und wird in die Lage versetzt, sich einen selbstkonfigurierten Kernel zu kompilieren und zu installieren. Wenn Sie so vorgehen, wie in diesem Kapitel beschrieben, bleibt der bisherige Kernel funktionsfähig und kann jederzeit auf Wunsch gebootet werden.

Kernel-Update 186
Die Kernelquellen 187
Konfiguration des Kernels 187
Kernel-Module 189
Einstellungen bei der Kernelkonfiguration 191
Übersetzen des Kernels 192
Kernel installieren 192
Festplatte nach der Übersetzung aufräumen 194

Der Kernel, der bei der Installation im /boot-Verzeichnis abgelegt wird, ist so konfiguriert, dass er ein möglichst breites Spektrum von Hardware unterstützt. Deshalb ist es *keineswegs erforderlich*, einen eigenen Kernel zu generieren, außer Sie wollen „experimentelle“ Features oder Treiber ausprobieren.

Zum Erzeugen eines neuen Kernels existieren bereits Makefiles, mit deren Hilfe der Ablauf fast völlig automatisiert ist. Lediglich die Auswahl der vom Kernel zu unterstützenden Hardware muss interaktiv durchlaufen werden. Da Sie Ihr Computer-System ziemlich gut kennen müssen, um eine funktionierende Auswahl zu treffen, empfehlen wir – wenigstens für die ersten Versuche – eine bestehende und funktionierende Konfigurationsdatei abzuändern und damit die Gefahr falscher Einstellungen zu vermindern.

Kernel-Update

Um einen SuSE Update-Kernel zu installieren, laden Sie das Update-Paket vom SuSE FTP-Server oder einem Mirror wie zum Beispiel: ftp://ftp.gwdg.de/pub/linux/suse/ herunter. Unter <version>_update/kernel liegen verschiedene Kernel-rpm. Mit k_deflt-⟨*version*⟩.i586.rpm wird der jeweilige Standard-Kernel bezeichnet. Vor der Installation sollten Sie den ursprünglichen Kernel und die dazugehörige initrd sichern. Geben Sie dazu als root die folgenden beiden Befehle ein:

```
cp /boot/vmlinuz /boot/vmlinuz.old
cp /boot/initrd /boot/initrd.old
```

Installieren Sie nun das neue Paket mit dem Befehl:

```
rpm -Uvh k_deflt-2.4.xxxxxx.rpm
```

Setzen Sie dabei die entsprechende Versionsnummer ein.

Ab SuSE Linux 7.3 wird reiserfs als Standardfilesystem verwendet, was den Einsatz einer „initial ramdisk“ voraussetzt. Diese wird mit dem Befehl mk_initrd neu geschrieben.

Um gegebenenfalls den alten Kernel booten zu können, muss dazu der Bootloader konfiguriert werden. Genaue Informationen dazu finden Sie im Kapitel *Booten und Bootmanager* auf Seite 85.

Um den Original-Kernel von den SuSE Linux CDs zu installieren, gehen Sie ähnlich vor. Auf CD 1 oder der DVD finden Sie im Verzeichnis boot den Standard Kernel als rpm-Paket. Installieren Sie diesen wie oben beschrieben. Falls Sie eine Fehlermeldung erhalten, dass bereits ein neueres Paket installiert ist, müssen Sie die Option --force beim rpm-Kommando zusätzlich angeben.

Die Kernelquellen

Um einen Kernel bauen zu können, müssen die Kernelquellen (Paket `kernel-source`) installiert werden. Andere erforderliche Pakete wie der C--Compiler (Paket `gcc`), die GNU Binutils (Paket `binutils`) und die Include-Dateien für den C-Compiler (Paket `glibc-devel`) werden dabei automatisch mitausgewählt.

Die Kernelquellen befinden sich nach der Installation im Verzeichnis `/usr/src/linux-<kernel-version>.SuSE`. Sollten Sie vorhaben, mit dem Kernel zu experimentieren und verschiedene Versionen des Kernels gleichzeitig auf der Platte zu halten, so bietet es sich an, die einzelnen Versionen in verschiedene Verzeichnisse zu entpacken und die augenblicklich relevanten Quellen über einen Link anzusprechen, da es Software-Pakete gibt, die die Kernelquellen unter `/usr/src/linux` erwarten. Diese Form der Installation wird von YaST2 automatisch vorgenommen.

Konfiguration des Kernels

Die Konfiguration des während der Installation oder während des Updates eingerichteten Kernel ist der Datei `/usr/src/linux/.config` zu entnehmen, wenn Sie noch nicht durch eine neue Konfiguration überschrieben worden ist. Wenn Sie die Konfiguration des aktuell betriebenen Kernels bearbeiten wollen, wechseln Sie als `root` in das Verzeichnis `/usr/src/linux` führen Sie zur Sicherheit folgenden Befehl aus:

```
erde:/usr/src/linux #  cp /boot/vmlinuz.config .config
```

Der Kernel kann entweder in der Kommandozeile, über ein Menü im Textmodus oder per Menü unter dem X Window System konfiguriert werden. Diese drei Wege werden im Folgenden kurz vorgestellt.

Tipp

Soll eine bereits vorhandene `.config` übernommen werden, ist es nur erforderlich, `make oldconfig` aufzurufen und fortzufahren wie in Abschnitt *Übersetzen des Kernels* auf Seite 192 beschrieben. Sie können bei dieser Methode die Konfiguration nicht anpassen.

Tipp

Kommandozeilenkonfiguration

Um den Kernel zu konfigurieren, wechseln Sie nach `/usr/src/linux` und geben folgenden Befehl ein: `make config`.

Sie werden nach einer Reihe von Systemfähigkeiten gefragt, die der Kernel unterstützen soll. Bei der Beantwortung der Fragen gibt es normalerweise zwei oder drei Möglichkeiten: Entweder einfaches (y) und (n), oder eine der drei Möglichkeiten (y) (engl. *yes*), (n) (engl. *no*) und (m) (engl. *module*). `'m'` bedeutet hierbei, dass der entsprechende Treiber nicht fest zum Kernel hinzugebunden wird, sondern vielmehr als Modul übersetzt wird, das zur Laufzeit zum Kernel hinzugeladen werden kann. Sämtliche Treiber, die zum Booten des Systems unbedingt benötigt werden, müssen fest zum Kernel hinzugebunden werden; in diesen Fällen also (y) wählen. Mit (Enter) bestätigen Sie die Vorauswahl, die aus der Datei `.config` eingelesen wird. Wenn Sie bei einer Frage eine andere Taste drücken, erhalten Sie einen kurzen Hilfetext zu der jeweiligen Option angezeigt.

Konfiguration im Textmodus

Angenehmer lässt sich die Konfiguration des Kernels mit „menuconfig“ durchführen; gegebenenfalls müssen Sie dazu das Paket `ncurses-devel` mit YaST2 nachinstallieren. Starten Sie die Kernel-Konfiguration mit dem Befehl `make menuconfig`.

Bei einer geringfügigen Änderung der Konfiguration müssen Sie sich hier nicht durch alle Fragen „durchtasten“, sondern können über das Menü direkt bestimmte Bereiche wählen. Die Voreinstellungen werden der Datei `.config` entnommen. Um eine andere Konfiguration zu laden, wählen Sie den Menüpunkt 'Load an Alternate Configuration File' und geben den Dateinamen an.

Konfiguration unter dem X Window System

Haben Sie das X Window System (Paket `xf86`) sowie Tcl/Tk (Paket `tcl` und Paket `tk`) installiert, so können Sie die Konfiguration alternativ durch

```
erde:/usr/src/linux #  make xconfig
```

vornehmen. Sie haben dann eine grafische Oberfläche, die das Konfigurieren komfortabler macht. Dazu müssen Sie das X Window System aber als Benutzer `root` gestartet haben oder in der Shell zuerst als normaler Benutzer `xhost +` eingeben, um `root` Zugriff auf das Display zu gewähren. Die Voreinstellungen werden aus der Datei `.config` ausgelesen. So lange Sie keine

neue Konfiguration erstellen, entsprechen die Einstellungen in dieser Datei dem SuSE Standard-Kernel.

Wenn Sie nur den SuSE-Kernel oder den derzeit benutzten Kernel modifizieren möchten, laden Sie die entsprechende Konfigurationsdatei durch Klick auf 'Load Configuration from File' im Hauptmenü und geben den Dateinamen an. Die Konfigurationsdatei für den gerade installierten Kernel ist `/boot/vmlinuz.config`. Um diese als Grundlage für Ihren neuen Kernel zu verwenden, kopieren Sie sie nach `/usr/src/linux/.config`.

Kernel-Module

Es gibt eine große Vielfalt an PC-Hardware-Komponenten. Um diese Hardware richtig benutzen zu können, braucht man einen „Treiber", über den das Betriebssystem (bei Linux der „Kernel") die Hardware richtig ansprechen kann. Generell gibt es zwei Mechanismen, Treiber in den Kernel zu integrieren:

- Die Treiber können fest zum Kernel dazugebunden sein. Solche Kernel „aus einem Stück" bezeichnen wir in diesem Buch auch als *monolithische* Kernel. Manche Treiber können nur in dieser Form verwendet werden.
- Die Treiber können erst bei Bedarf in den Kernel geladen werden, der in diesem Fall als *modularisierter* Kernel bezeichnet wird. Das hat den Vorteil, dass wirklich nur die benötigten Treiber geladen sind und dass der Kernel keinen unnötigen Ballast enthält.

Welche Treiber fest zum Kernel gebunden und welche als Module realisiert werden, wird bei der Konfiguration des Kernels festgelegt. Alle Kernel-Komponenten, die nicht zwingend während des Bootvorgangs benötigt werden, sollten als Modul realisiert werden. So wird sichergestellt, dass der Kernel nicht zu groß wird und dass der Kernel ohne Schwierigkeiten vom BIOS und einem beliebigen Bootloader geladen werden kann. Der Festplatten-Treiber, Unterstützung für `ext2` und ähnliche Dinge sind also im Regelfall direkt in den Kernel hineinzukompilieren, Unterstützung für `isofs`, `msdos` oder `sound` sollten in jedem Fall als Module kompiliert werden.

Die Kernelmodule werden in dem Verzeichnis `/lib/modules/`⟨*Version*⟩ abgelegt, wobei ⟨*Version*⟩ der momentanen Version des Kernels entspricht (beispielsweise 2.4.18).

Umgang mit Modulen

Folgende Befehle zum Umgang mit Modulen stehen zur Verfügung:

- `insmod`
  Mit dem Befehl insmod wird das angegebene Modul geladen. Das Modul wird in einem Unterverzeichnis von `/lib/modules/`⟨*Version*⟩ gesucht. Zugunsten von `modprobe` (s. u.) sollte `insmod` *nicht* mehr verwendet werden.

- `rmmod`
  Entlädt das angegebene Modul. Dies ist natürlich nur dann möglich, wenn die entsprechende Funktionalität des Kernels nicht mehr verwendet wird. So ist es nicht möglich, das Modul `isofs` zu entladen, wenn noch eine CD gemountet ist.

- `depmod`
  Dieser Befehl erzeugt eine Datei mit dem Namen `modules.dep` im Verzeichnis `/lib/modules/`⟨*Version*⟩, in der die Abhängigkeiten der einzelnen Module untereinander verzeichnet sind. Damit stellt man sicher, dass beim Laden eines Modules alle davon abhängigen Module ebenfalls automatisch geladen werden. Die Datei mit den Modul-Abhängigkeiten beim Start des Systems automatisch generiert, sofern sie noch nicht existiert.

- `modprobe`
  Laden bzw. Entladen eines Modules mit Berücksichtigung der Abhängigkeiten von anderen Modulen. Dieser Befehl ist sehr mächtig und kann für eine Reihe weiterer Zwecke eingesetzt werden (etwa Durchprobieren aller Module eines bestimmten Typs, bis eines erfolgreich geladen werden kann). Im Gegensatz zum Laden mittels insmod wertet modprobe die Datei `/etc/modules.conf` aus und sollte daher generell zum Laden von Modulen verwendet werden. Für eine ausführliche Erklärung sämtlicher Möglichkeiten lesen Sie bitte die zugehörigen Manual-Pages.

- `lsmod`
  Zeigt an, welche Module gegenwärtig geladen sind und von wie vielen anderen Modulen sie verwendet werden. Module, die vom Kernel-Daemon geladen wurden, sind durch ein nachfolgendes `autoclean` gekennzeichnet. Die Kennzeichnung mit `autoclean` weist darauf hin, dass diese Module automatisch wieder entfernt werden, wenn sie längere Zeit nicht benutzt wurden und man entsprechende Vorkehrungen getroffen hat; vgl. jedoch auf der nächsten Seite.

- modinfo
  Zeigt Informationen zu einem Modul an.

/etc/modules.conf

Das Laden von Modulen wird über die Datei /etc/modules.conf beeinflusst; vgl. Manual-Page von depmod (man depmod).

Insbesondere können in dieser Datei die Parameter für solche Module eingetragen werden, die direkt auf die Hardware zugreifen und daher auf das spezifische System eingestellt werden müssen (z. B. CD-ROM-Treiber oder Netzwerktreiber). Die hier eingetragenen Parameter sind im Prinzip identisch mit denen, die am Bootprompt des Kernels (z. B. von LILO) übergeben werden, jedoch weichen in vielen Fällen die Namen von denen ab, die am Bootprompt zum Einsatz kommen. Wenn das Laden eines Moduls nicht erfolgreich ist, versuchen Sie, in dieser Datei die Hardware zu spezifizieren und verwenden Sie zum Laden des Moduls modprobe anstelle von insmod.

Kmod – der Kernel Module Loader

Der eleganteste Weg bei der Verwendung von Kernel-Modulen ist der Einsatz des „Kernel Module Loader“. Kmod wacht im Hintergrund und sorgt dafür, dass benötigte Module durch modprobe-Aufrufe automatisch geladen werden, sobald auf die entsprechende Funktionalität des Kernels zugegriffen wird.

Um den Kmod verwenden zu können, müssen Sie bei der Kernel-Konfiguration die Option ‘Kernel module loader’ (CONFIG_KMOD) aktivieren.

Der Kmod ist nicht dafür ausgelegt, Module wieder automatisch zu entladen; bei der heutigen RAM-Ausstattung der Rechner wäre der Gewinn an Arbeitsspeicher nur marginal; vgl. auch /usr/src/linux/Documentation/kmod.txt. Server-Maschinen, die spezielle Aufgaben zu erfüllen haben und nur wenige Treiber benötigen, werden aus Performance-Gründen einen „monolithischen“ Kernel bevorzugen.

Einstellungen bei der Kernelkonfiguration

Die einzelnen Konfigurationsmöglichkeiten des Kernels können hier nicht im Detail dargestellt werden. Machen Sie bitte Gebrauch von den zahlreich vorhandenen Hilfetexten zur Kernel-Konfiguration. Der neueste Stand der Dokumentation findet sich immer im Verzeichnis /usr/src/linux/Documentation.

Übersetzen des Kernels

Wir empfehlen, ein „bzImage“ zu generieren. So lässt es sich in der Regel umgehen, dass der Kernel „zu groß“ wird, wie dies leicht passieren kann, wenn man zu viele Features auswählt und ein „zImage“ herstellt (typisch sind dann die Meldungen "kernel too big" oder "System is too big").

Nachdem Sie den Kernel für Ihre Gegebenheiten konfiguriert haben, starten Sie die Kompilation:

```
erde:/usr/src/linux #  make dep
erde:/usr/src/linux #  make clean
erde:/usr/src/linux #  make bzImage
```

Diese 3 Befehle können Sie auch in einer Befehlszeile eingeben:

```
erde:/usr/src/linux #  make dep clean bzImage
```

Nach der erfolgreichen Übersetzung finden Sie den komprimierten Kernel in `/usr/src/linux/arch/i386/boot`. Das Kernel-Image – die Datei, die den Kernel enthält – heißt `bzImage`. Finden Sie diese Datei nicht vor, ist aller Wahrscheinlichkeit nach ein Fehler während der Kernelübersetzung aufgetreten. Unter der Bash können Sie mit

```
erde:/usr/src/linux #  make bzImage 2>&1 | tee kernel.out
```

den Kompilationsvorgang erneut starten und in die Datei `kernel.out` „mitschreiben“ lassen.

Wenn Sie Teile des Kernels als ladbare Module konfiguriert haben, müssen Sie anschließend das Übersetzen dieser Module veranlassen. Dies erreichen Sie durch

```
erde:/usr/src/linux #  make modules
```

Kernel installieren

Nachdem Sie den Kernel übersetzt haben, müssen Sie dafür sorgen, dass dieser neue Kernel installiert wird, um ihn künftig booten zu können. Wenn Sie LILO verwenden, so muss dies gleichfalls neu installiert werden. Im einfachsten Fall kopieren Sie dazu den neuen Kernel nach `/boot/vmlinuz` und rufen dann LILO auf; um sich vor unliebsamen Überraschungen zu schützen, empfiehlt es sich jedoch, den alten Kernel zunächst beizubehalten (als

/boot/vmlinuz.old), um ihn notfalls booten zu können, wenn der neue Kernel nicht wie erwartet funktioniert:

```
erde:/usr/src/linux #  cp /boot/vmlinuz /boot/vmlinuz.old
erde:/usr/src/linux #  cp arch/i386/boot/bzImage /boot/vmlinuz
erde:/usr/src/linux #  lilo
```

Das Makefile-Target `make bzlilo` erledigt diese 3 Schritte übrigens in einem Rutsch.

Die übersetzten Module müssen nun noch installiert werden; durch Eingabe von

```
erde:/usr/src/linux #  make modules_install
```

können Sie diese in die korrekten Zielverzeichnisse unter `/lib/modules/`⟨*Version*⟩ kopieren lassen. Dabei werden die alten Module bei gleicher Kernelversion überschrieben; Sie können jedoch die ursprünglichen Module zusammen mit dem Kernel von den CDs wieder installieren.

Tipp

Es ist darauf zu achten, dass Module, deren Funktionalität man jetzt eventuell direkt in den Kernel einkompiliert hat, unter `/lib/modules/`⟨*Version*⟩ entfernt werden. Sonst kann es zu unvorhersehbaren Effekten kommen! Dies ist ein Grund, weshalb dem Ungeübten vom Selbstkompilieren des Kernels *dringend* abgeraten wird.

Tipp

Damit der alte Kernel von LILO (jetzt `/boot/vmlinuz.old`) gebootet werden kann, tragen Sie in der Datei `/etc/lilo.conf` zusätzlich ein Label `Linux.old` als Boot-Image ein. Dieses Vorgehen wird ausführlich im Kapitel *Booten und Bootmanager* auf Seite 85 beschrieben. Haben Sie die Datei `/etc/lilo.conf` nach Ihren Wünschen angepasst, so müssen Sie erneut `lilo` aufrufen.

Falls Sie Linux von DOS aus über `linux.bat` – also mit `loadlin` – starten, müssen Sie den neuen Kernel noch nach `/dosc/loadlin/bzimage` bzw. dorthin, wohin Sie das Verzeichnis `loadlin` haben installieren lassen, kopieren, damit er beim nächsten Booten wirksam werden kann.

Falls Sie Linux über den Windows NT Bootmanager starten, dürfen Sie nun nicht vergessen, erneut den LILO-Bootsektor umzukopieren (vgl. Abschnitt *Windows NT, 2000 oder XP und Linux* auf Seite 105).

Weiterhin ist Folgendes zu beachten: Die Datei `/boot/System.map` enthält die Kernelsymbole, die die Kernelmodule benötigen, um Kernelfunktionen korrekt aufrufen zu können. Diese Datei ist abhängig vom aktuellen Kernel. Daher sollten Sie nach der Übersetzung und Installation des Kernels die aktuelle Datei `/usr/src/linux/System.map` in das Verzeichnis `/boot` kopieren. Bei jeder Kernelübersetzung wird diese Datei neu erzeugt. Falls Sie Ihren Kernel mittels `make bzlilo` bzw. `make zlilo` erstellen, wird diese Aufgabe automatisch für Sie erledigt.

Sollten Sie beim Booten eine Fehlermeldung wie "System.map does not match actual kernel" erhalten, dann wurde wahrscheinlich nach der Kernelübersetzung die Datei `System.map` nicht nach `/boot` kopiert.

Festplatte nach der Übersetzung aufräumen

Sie können die während der Kernel-Übersetzung erzeugten Objekt-Dateien löschen, falls Sie Probleme mit dem Plattenplatz haben:

```
erde:~ #  cd /usr/src/linux
erde:/usr/src/linux #  make clean
```

Falls Sie jedoch über ausreichend Plattenplatz verfügen und vorhaben, den Kernel des Öfteren neu zu konfigurieren, so überspringen Sie diesen letzten Schritt. Ein erneutes Übersetzen des Kernels ist dann erheblich schneller, da nur die Teile des Systems neu übersetzt werden, die von den entsprechenden Änderungen betroffen sind.

Systemmerkmale

Hinweise zu *Filesystem Hierarchy Standard* (FHS) und *Linux Standard Base* (LSB), einzelen Softwarepaketen und besonderen Merkmalen wie dem Booten mit der „initrd“, dem Programm linuxrc und dem „Rettungssystem“.

Linux-Standards 196
Beispiel-Umgebungen für FTP und HTTP 196
Hinweise zu speziellen Softwarepaketen 197
Booten mit der initial ramdisk 202
linuxrc 207
Das SuSE Rettungssystem 212
Virtuelle Konsolen 219
Tastaturbelegung 219
Lokale Anpassungen – I18N/L10N 220

Linux-Standards

Filesystem Hierarchy Standard (FHS)

SuSE Linux strebt eine weitgehende Konformität zum *Filesystem Hierarchy Standard* (FHS, Paket `fhs`) an; vgl. `http://www.pathname.com/fhs/`. Aus diesem Grunde ist es bisweilen erforderlich, Dateien oder Verzeichnisse an die „richtigen" Plätze zu verschieben, wie diese im FHS festgelegt sind.

Linux Standard Base (LSB)

SuSE unterstützt aktiv die Bemühungen des *Linux Standard Base*-Projekts; aktuelle Informationen dazu unter `http://www.linuxbase.org`.

Die LSB-Spezifikation liegt in der Version 1.2 vor; nunmehr ist der Filesystem Hierarchy Standard (FHS) Teil der Spezifikation und es sind u. a. das Paketformat und die Initialisierung des Systems festgelegt; vgl. Kapitel *Das Bootkonzept* auf Seite 225.

teTeX – TeX unter SuSE Linux

TeX ist ein komplexes Satzsystem, das auf zahlreichen Plattformen läuft. Es ist über Makro-Pakete wie LaTeX erweiterbar. Es besteht aus sehr vielen einzelnen Dateien, die gemäß der *TeX Directory Structure* (TDS) zusammenzustellen sind (vgl. `ftp://ftp.dante.de/tex-archive/tds/`) teTeX ist eine Zusammenstellung aktueller TeX-Software.

Unter SuSE Linux kommt teTeX in einer Konfiguration zum Einsatz, die sowohl die Anforderungen des TDS als auch des FHS erfüllt.

Beispiel-Umgebungen für FTP und HTTP

Zu FTP

Um die Einrichtung eines FTP-Servers zu erleichtern, hält das Paket `ftpdir` eine Beispiel-Umgebung bereit. Diese Umgebung wird unter `/srv/ftp` installiert.

Zu HTTP

Apache ist der Standard-Webserver bei SuSE Linux; gleichzeitig mit der Installation des Apache werden Beispiel-Dokumente unter `/srv/httpd` zur Verfügung gestellt. Wenn Sie einen eigenen Webserver aufbauen wollen, tragen Sie bitte eine eigene `DocumentRoot` in `/etc/httpd/httpd.conf` ein und legen Sie dort Ihre Dateien (Dokumente, Bilder etc.) ab.

Hinweise zu speziellen Softwarepaketen

Paket bash und /etc/profile

In dieser Reihefolge wertet die bash die Initialisierungsdateien aus, wenn sie als Loginshell aufgerufen wird:

1. `/etc/profile`
2. `~/.profile`
3. `/etc/bash.bashrc`
4. `~/.bashrc`

Eigene Einträge können Benutzer in `~/.profile` bzw. `~/.bashrc` vornehmen. Um ordnungsgemäßes Abarbeiten dieser Dateien zu gewährleisten, ist es erforderlich, dass die aktuellen Grundeinstellungen von `/etc/skel/.profile` bzw. `/etc/skel/.bashrc` in das Benutzerverzeichnis übernommen werden. Nach einem Update empfiehlt sich deshalb die Einstellungen aus `/etc/skel` zu übernehmen; um keine eigenen Anpassungen zu verlieren, führen Sie bitte die folgenden Shellbefehle aus:

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

Danach sind die eigenen Anpassungen aus den Dateien `*.old` zurückzuschreiben.

Paket cron

Die cron-Tabellen liegen unter `/var/spool/cron/tabs`. Als systemweite Tabelle wird die Datei `/etc/crontab` eingerichtet. In der Datei `/etc/crontab` muss zusätzlich nach der Zeitangabe eingetragen werden, unter welchem Benutzer der jeweilige Auftrag ausgeführt werden soll (vgl. Datei 11, dort ist `root` angegeben); dem gleichen Format folgen paketspezifische Tabellen, die in `/etc/cron.d` liegen – vgl. Manual-Page von `cron` (`man 8 cron`).

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

Datei 11: *Beispiel eines Eintrags in /etc/crontab*

`/etc/crontab` kann *nicht* mit `crontab -e` bearbeitet werden, sondern muss direkt in einen Editor geladen, bearbeitet und schließlich gespeichert werden.

Einige Pakete installieren in den Verzeichnissen `/etc/cron.hourly`, `/etc/cron.daily`, `/etc/cron.weekly` und `/etc/cron.monthly` Shellskripten, deren Abarbeitung von `/usr/lib/cron/run-crons` gesteuert wird. `/usr/lib/cron/run-crons` wird alle 15 Minuten von der Haupt-Tabelle (`/etc/contrab`) aufgerufen; so wird sichergestellt, dass eventuell versäumte Läufe rechtzeitig nachgeholt werden. Wundern Sie sich also bitte nicht, wenn kurz nach dem Booten der Benutzer `nobody` in der Prozess-Tabelle mit regen Aktivitäten auftaucht; `nobody` aktualisiert wahrscheinlich dann gerade die locate-Datenbank (vgl. Abschnitt *Einstellungen in den Dateien in /etc/sysconfig* auf Seite 251).

Die täglichen Wartungsarbeiten am System sind aus Gründen der Übersichtlichkeit auf mehrere Skripten verteilt worden (Paket Paket `aaa_base`). In `/etc/cron.daily` gibt es also neben `aaa_base` z. B. die Komponenten `backup-rpmdb`, `clean-tmp` oder `clean-vi`.

Protokoll-Dateien – das Paket logrotate

Zahlreiche System-Dienste („Daemons") und auch der Kernel selber protokollieren regelmäßig Systemzustände oder besondere Vorkommnisse in Protokoll-Dateien (engl. *logfiles*). So kann der Administrator zuverlässig feststellen, in welchem Zustand sich das System zu einem bestimmten Zeitpunkt befand, Fehler oder Fehlfunktionen erkennen und gezielt beheben. Diese Protokoll-Dateien werden in der Regel gemäß FHS unter `/var/log` abgelegt und werden von Tag zu Tag größer. Mit Hilfe Paketes Paket `logrotate` ist es möglich, das Wachsen der Protokoll-Dateien zu steuern.

Umstellung auf logrotate (8.0)

Beim Update einer Version vor SuSE Linux 8.0 werden alte Einstellungen übernommen:

- Einträge aus `/etc/logfile`, die keinem speziellen Paket zugeordnet sind, werden nach `/etc/logrotate.d/aaa_base` verschoben.
- Die ehemalige `rc.config`-Variable `MAX_DAYS_FOR_LOG_FILES` wird als `dateext` und `maxage` in der Konfigurationsdatei abgebildet; vgl. Manual-Page von `logrotate` (`man 8 logrotate`) abgebildet.

Konfiguration

In der Konfigurationsdatei `/etc/logrotate.conf` wird das generelle Verhalten festgelegt. Mit der `include`-Angabe wird insbesondere konfiguriert, welche weiteren Dateien ausgewertet werden sollen; bei SuSE Linux ist vorgesehen, dass die einzelnen Pakete in `/etc/logrotate.d` Dateien installieren (beispielsweise `syslog` oder `yast`).

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we’ll rotate them here
#/var/log/wtmp {
#    monthly
#    create 0664 root utmp
#    rotate 1
#}

# system-specific logs may be also be configured here.
```

Datei 12: *Beispiel für /etc/logrotate.conf*

logrotate selbst wird über cron gesteuert; es wird einmal täglich von `/etc/cron.daily/logrotate` angestoßen.

Hinweis

Die Option `create` liest etwaige Einstellungen ein, die Sie als Administrator in den Dateien `/etc/permissions*` vorgenommen haben könnten. Stellen Sie bitte sicher, dass es bei eigenen Anpassungen zu keinen Konflikten kommt.

Hinweis

Manual-Pages

Für einige GNU-Programme (z. B. tar) werden die Manual-Pages nicht mehr weiter gepflegt. An ihre Stelle treten als Schnellübersicht die `--help`-Ausgabe sowie als ausführliche Manuals die Info-Dateien. Info (`info`) ist GNUs Hypertext-System. Mit `info info` erhält man erste Hilfe zur Benutzung; `info` kann entweder über Emacs `emacs -f info` aufgerufen werden, oder standalone: `info`. Angenehm zu bedienen sind `tkinfo`, `xinfo` oder der Zugriff über das Hilfesystem.

Der Befehl ulimit

Mit dem Befehl `ulimit` (engl. *user limits*) ist es möglich, Limits für die Nutzung von Systemressourcen zu setzen, bzw. sich diese anzeigen zu lassen. Insbesondere ist `ulimit` dazu geeignet, den zur Verfügung stehenden Speicher für Anwendungen zu begrenzen. Dadurch kann verhindert werden, dass eine Anwendung übermäßig viel (allen) Speicherplatz für sich beschlagnahmt und dass das System so zum Stillstand kommen könnte.

Der Aufruf von `ulimit` kann mit verschiedenen Optionen geschehen. Um den Speicherverbrauch zu begrenzen, sind z. B. die Optionen in Tabelle 10.1 tauglich.

`-m`	max. Größe des physikalischen Speichers
`-v`	max. Größe des virtuellen Speichers (Swap)
`-s`	max. Größe des Stacks
`-c`	max. Größe der Core-Dateien
`-a`	Anzeige der gesetzten Limits

Tabelle 10.1: `ulimit`*: Ressourcen für den Anwender einstellen*

Systemweit können die Einstellungen in /etc/profile vorgenommen werden. Dort muss beispielsweise das Erzeugen von Core-Dateien freigeschaltet werden, die Programmierer zum „Debuggen“ benötigen. Als Anwender kann man die vom Systemadministrator in /etc/profile vorgegebenen Werte nicht erhöhen, aber man kann spezielle Einstellung in die eigene ~/.bashrc eintragen.

```
# Begrenzung des realen Speichers:
ulimit -m 98304

# Begrenzung des virtuellen Speichers:
ulimit -v 98304
```

Datei 13: *ulimit-Einstellungen in ~/.bashrc*

Die Speicherangaben müssen in KB gemacht werden. Für detailliertere Informationen werfen Sie bitte einen Blick in die Manual-Page von bash (man bash).

Hinweis

Nicht alle Shells unterstützen ulimit-Angaben. Wenn Sie auf übergreifende Einstellungen für derartige Beschränkungen angewiesen sind, dann bietet PAM (z. B. pam_limits) weitgehende Einstellmöglichkeiten.

Hinweis

Der Befehl free

Der Befehl free ist etwas irreführend, wenn es darum geht herauszufinden, wie der Arbeitsspeicher gerade verwendet wird…

Die nützlichen Informationen findet man in /proc/meminfo. Heutzutage sollte sich eigentlich kein Anwender darum Gedanken machen, dem ein modernes Betriebssystem wie Linux zur Verfügung steht. Das Konzept vom „freien Arbeitsspeicher“ datiert von der Zeit her, als es noch keine vereinheitlichte Speicherverwaltung (engl. *unified memory management*) gab – unter Linux gilt das Motto: *freier Speicher ist schlechter Speicher* (engl. *free memory is bad memory*). Infolgedessen ist Linux immer bestrebt, verschiedene Caches auszubalancieren, nie aber wirklich freien (= ungenutzten) Speicher zuzulassen.

Der Kernel weiß im Grunde nichts direkt von Programmen oder Benutzerdaten; er verwaltet Programme und Benutzerdaten im so genannten „Page

Cache“. Wenn der Speicher knapp wird, werden Teile davon entweder in den Swapbereich oder in die Dateien geschrieben, aus denen sie ursprünglich mit Hilfe des Systemaufrufs `mmap` gelesen wurden; vgl. Manual-Page von `mmap` (`man 2 mmap`).

Des Weiteren hält der Kernel auch noch andere Zwischenspeicher, wie den „slab cache“, der z. B. die für den Netzwerkzugriff benutzten Puffer enthält. Dadurch werden eventuelle Differenzen zwischen den Zählern in `/proc/meminfo` erklärt. Die meisten, aber nicht alle, sind über `/proc/slabinfo` abfragbar.

Die /etc/resolv.conf

Die Namensauflösung wird über die Datei `/etc/resolv.conf` geregelt; vgl. Abschnitt *DNS – Domain Name Service* auf Seite 297.

Diese Datei wird stets nur von dem Skript `/sbin/modify_resolvconf` aktualisiert. Es ist keinem Programm erlaubt, `/etc/resolv.conf` direkt zu manipulieren. Nur wenn diese Regel beachtet wird, kann sichergestellt werden, dass die Netzwerkkonfiguration und zugehörigen Daten konsistent gehalten werden.

Booten mit der initial ramdisk

Problemstellung

Sobald der Linux-Kernel geladen ist und das Root-Dateisystem (`/`) gemountet hat, können Programme ausgeführt und weitere Kernel-Module eingebunden werden, um zusätzliche Funktionalitäten bereitzustellen.

Um aber das Root-Dateisystem überhaupt mounten zu können, müssen verschiedene Bedigungenen erfüllt sein: Der Kernel benötigt die entsprechenden Treiber, um das Gerät ansprechen zu können, auf dem das Root-Dateisystem liegt (insbesondere SCSI-Treiber). Weiter muss der Kernel den Code enthalten, der benötigt wird, um das Dateisystem lesen zu können (`ext2`, `reiserfs`, `romfs` usw.). Weiterhin ist es denkbar, dass bereits das Root-Dateisystem verschlüsselt ist; zum Mounten ist in diesem Fall die Eingabe des Schlüssels/Passworts erforderlich.

Betrachtet man nur einmal das Problem der SCSI-Treiber, so sind verschiedene Lösungsansätze denkbar: Der Kernel kann alle denkbaren Treiber enthalten. Problematisch, da sich verschiedene Treiber „beißen“ können; außerdem wird der Kernel dadurch sehr groß. Eine andere Möglichkeit besteht darin,

verschiedene Kernel zur Verfügung zu stellen, die jeweils nur einen oder sehr wenige SCSI-Treiber enthalten. Auch dieser Weg ist problematisch, da er eine sehr große Zahl unterschiedlicher Kernel notwendig macht. Ein Problem, das durch verschieden optimierte Kernel (Pentium-Optimierung, SMP) noch weiter verschärft wird.

Der Ansatz, den SCSI-Treiber als Modul zu laden, führt zur generellen Problematik, der durch das Konzept der *initial ramdisk* begegnet wird: Das Schaffen einer Möglichkeit, Userspace-Programme bereits vor dem Mounten des Root-Dateisystems ausführen zu können.

Konzept der initial ramdisk

Die *initial ramdisk* (auch „initdisk" oder „initrd" genannt) löst genau diese oben beschriebenen Probleme. Der Linux-Kernel bietet die Möglichkeit, ein (kleines) Dateisystem in eine Ramdisk laden zu lassen, und darin Programme ausführen zu lassen, bevor das eigentliche Root-Dateisystem gemountet wird. Das Laden der `initrd` wird dabei vom Bootloader (LILO, loadlin usw.) übernommen; all diese Bootloader benötigen lediglich BIOS-Routinen, um Daten vom Bootmedium zu laden. Wenn der Bootloader den Kernel laden kann, dann kann er auch die initial ramdisk laden. Spezielle Treiber sind somit nicht erforderlich.

Ablauf des Bootvorgangs mit initrd

Der Bootloader lädt den Kernel und die `initrd` in den Speicher und startet den Kernel, wobei der Bootloader dem Kernel mitteilt, dass eine `initrd` vorhanden ist und wo im Speicher diese liegt.

War die `initrd` komprimiert (was typischerweise der Fall ist), so dekomprimiert der Kernel die `initrd` und mountet sie als temporäres Root-Dateisystem. Hierauf wird in der `initrd` ein Programm mit dem Namen linuxrc gestartet. Dieses Programm kann nun all die Sachen tun, die erforderlich sind, um das richtige Root-Dateisystem mounten zu können. Sobald linuxrc terminiert, wird die (temporäre) `initrd` wieder abgehängt (engl. *unmounted*) und der Bootvorgang wird wie gewohnt mit dem Mounten des richtigen Root-Dateisystems fortgeführt. Das Mounten der `initrd` und das Ausführen von linuxrc kann somit als ein kurzes Intermezzo während eines normalen Bootvorgangs betrachtet werden.

Der Kernel versucht nach dem Booten der tatsächlichen Root-Partition die `initrd` auf das Verzeichnis `/initrd` umzumounten. Wenn das fehlschlägt, weil z. B. der Mountpunkt `/initrd` nicht vorhanden ist, wird der Kernel

versuchen, die initrd abzuhängen. Sollte auch dies fehlschlagen, ist das System zwar voll funktionsfähig, jedoch kann der durch die initrd belegte Speicher nie freigegeben werden und steht somit nicht mehr zur Verfügung.

Das Programm linuxrc

Für das Programm linuxrc in der initrd gibt es lediglich die folgenden Anforderungen: Es muss den speziellen Namen linuxrc tragen und es muss im Root-Verzeichnis der initrd liegen. Abgesehen davon muss es lediglich vom Kernel ausgeführt werden können. Das bedeutet, dass linuxrc durchaus dynamisch gelinkt sein darf; in diesem Fall müssen natürlich die „shared libraries" wie gewohnt vollständig unter /lib in der initrd verfügbar sein. Weiter darf linuxrc auch ein Shellskript sein; in diesem Fall muss natürlich eine Shell in /bin existieren. Kurz gesagt, muss die initrd ein minimales Linux-System enthalten, das die Ausführung des Programmes linuxrc erlaubt. Bei der Installation von SuSE Linux wird ein statisch gelinktes linuxrc verwendet, um die initrd so klein wie möglich halten zu können (der Platz auf Bootdisketten ist sehr knapp). linuxrc wird mit root-Rechten ausgeführt.

Das echte Root-Dateisystem

Sobald linuxrc terminiert, wird die initrd abgehängt und verworfen, der Bootvorgang geht normal weiter und der Kernel mountet das wirkliche Root-Dateisystem. Was als Root-Dateisystem gemountet werden soll, kann durch linuxrc beeinflusst werden. Dazu muss linuxrc lediglich das /proc-Dateisystem mounten und den Wert des echten Root-Dateisystems in numerischer Form nach /proc/sys/kernel/real-root-dev schreiben.

Bootloader

Die meisten Bootloader (vor allem LILO, loadlin und syslinux) können mit initrd umgehen. Die einzelnen Bootloader werden wie folgt angewiesen, eine initrd zu verwenden:

LILO Eintrag der folgenden Zeile in /etc/lilo.conf:

```
initrd=/boot/initrd
```

Die Datei /boot/initrd ist die *initial ramdisk*. Sie kann (muss aber nicht) komprimiert sein.

loadlin.exe Aufruf mittels:

```
C:> loadlin ⟨kernelimage⟩ initrd=C:\loadlin\initrd ⟨parameter⟩
```

syslinux Eintrag der folgenden Zeile in `syslinux.cfg`:

```
append initrd=initrd ⟨weitere Parameter⟩
```

Anwendung von initrd bei SuSE

Installation des Systems

Die `initrd` wird bereits seit geraumer Zeit für die Installation verwendet: Dabei kann der Anwender in linuxrc Module laden und die für eine Installation notwendigen Eingaben (wie vor allem Quellmedium) machen. Linuxrc startet dann YaST, das die Installation durchführt. Hat YaST seine Arbeit getan, teilt es linuxrc mit, wo das Root-Dateisystem des frisch installierten Systems liegt. linuxrc schreibt diesen Wert nach `/proc`, beendet sich, und der Kernel bootet in das frisch installierte System weiter.

Bei einer Installation von SuSE Linux bootet man somit von Anfang an quasi das System, das gerade erst installiert wird – irgendwie schick. Ein echter Reboot nach der Installation erfolgt nur, wenn der gerade laufende Kernel nicht zu den Modulen passt, die im System installiert wurden. Da SuSE Linux derzeit bei der Installation einen Kernel für Uni-Prozessor-Systeme verwendet, geschieht dies derzeit nur dann, wenn im System ein SMP-Kernel mitsamt entsprechenden Modulen installiert wurde. Um alle Module verwenden zu können, muss deshalb der neu im System installierte SMP-Kernel gebootet werden.

Booten des installierten Systems

In der Vergangenheit hat YaST mehr als 40 Kernel für die Installation im System angeboten, wobei sich die Kernel im Wesentlichen dadurch unterschieden hatten, dass jeder Kernel einen bestimmten SCSI-Treiber enthielt. Dies war nötig, um nach dem Booten das Root-Dateisystem mounten zu können. Weitere Treiber konnten dann als Modul nachgeladen werden.

Da inzwischen aber auch optimierte Kernel zur Verfügung gestellt werden, ist dieses Konzept nicht mehr tragbar – es wären inzwischen weit über 100 Kernel-Images nötig.

Daher wird nun auch für das normale Starten des Systems eine `initrd` verwendet. Die Funktionsweise ist analog wie bei einer Installation. Das hier eingesetzte linuxrc ist jedoch einfach nur ein Shellskript, das lediglich die Aufgabe hat, einige vorgegebene Module zu laden. Typischerweise handelt es sich nur um ein einziges Modul, nämlich denjenigen SCSI-Treiber, der benötigt wird, um auf das Root-Dateisystem zugreifen zu können.

Erstellen einer initrd

Das Erstellen einer `initrd` erfolgt mittels des Skripts `mkinitrd` (früher `mk_initrd`). Die zu ladenden Module werden bei SuSE Linux durch die Bezeichner `INITRD_MODULES` in `/etc/sysconfig/kernel` festgelegt. Nach einer Installation wird diese Variable automatisch durch die richtigen Werte vorbelegt (das Installations-linuxrc weiß ja, welche Module geladen wurden). Dabei ist zu erwähnen, dass die Module in genau der Reihenfolge geladen werden, in der sie in `INITRD_MODULES` auftauchen. Das ist besonders wichtig, wenn mehrere SCSI-Treiber verwendet werden, da sich ansonsten die Benennung der Platten ändern würde. Streng genommen würde es reichen, nur denjenigen SCSI-Treiber laden zu lassen, der für den Zugriff auf das Root-Dateisystem benötigt wird. Da das automatische Nachladen zusätzlicher SCSI-Treiber jedoch problematisch ist (wie sollte es „getriggert" werden, wenn auch am zweiten SCSI-Adapter Platten hängen), laden wir alle bei der Installation verwendeten SCSI-Treiber mittels der `initrd`.

Das aktuelle `mkinitrd` prüft, ob für den Zugriff auf das Root-Dateisystem überhaupt ein SCSI-Treiber benötigt wird. Ruft man `mkinitrd` auf einem System auf, bei dem `/` auf EIDE-Platten liegt, erstellt es keine `initrd`, da diese nicht nötig ist, weil die bei SuSE Linux verwendeten Kernel bereits die EIDE-Treiber enthalten. Da inzwischen immer mehr spezielle EIDE-Controller auf den Markt kommen, wird es aber voraussichtlich für die Zukunft nötig werden, auch in diesen Fällen eine `initrd` für das Booten des installierten Systems zu verwenden.

Wichtig: Da das Laden der `initrd` durch den Bootloader genauso abläuft wie das Laden des Kernels selbst (LILO vermerkt in seiner `map`-Datei die Lage der Dateien), muss nach jeder Änderung der `initrd` der Bootloader neu installiert werden!

Mögliche Schwierigkeit – Selbstcompilierte Kernel

Übersetzt man sich selbst einen Kernel, so kann es zu folgendem häufigen Problem kommen: Aus Gewohnheit wird der SCSI-Treiber fest in den Kernel gelinkt, die bestehende `initrd` bleibt aber unverändert. Beim Booten ge-

schieht nun folgendes: Der Kernel enthält bereits den SCSI-Treiber, die Hardware wird erkannt. Die `initrd` versucht nun jedoch, den Treiber nochmals als Modul zu laden; dies führt bei einigen SCSI-Treibern (insbesondere beim `aic7xxx`) zum Stillstand des Systems. Streng genommen handelt es sich um einen Kernelfehler (ein bereits vorhandener Treiber darf nicht ein zweites Mal als Modul geladen werden können) – das Problem ist aber bereits in anderem Zusammenhang bekannt (serieller Treiber).

Es gibt mehrere Lösungen für das Problem: Entweder den Treiber als Modul konfigurieren (dann wird er korrekt in der `initrd` geladen), oder aber den Eintrag für die `initrd` aus `/etc/lilo.conf` entfernen. Äquivalent zur letzteren Lösung ist es, den Treiber aus `INITRD_MODULES` zu entfernen und `mkinitrd` aufzurufen, das dann feststellt, dass keine `initrd` benötigt wird.

Ausblick

Für die Zukunft ist es denkbar, dass eine `initrd` für weitaus mehr (und anspruchsvollere) Dinge verwendet wird als nur für das Laden der Module, die für den Zugriff auf `/` benötigt werden.

- „High end“ EIDE-Treiber
- Root-Dateisystem auf Software RAID (linuxrc setzt die `md`-Devices auf)
- Root-Dateisystem auf LVM
- Root-Dateisystem ist verschlüsselt (linuxrc fragt nach Passwort)
- Root-Dateisystem auf einer SCSI-Platte am PCMCIA-Adapter

Weitere Informationen

`/usr/src/linux/Documentation/ramdisk.txt`
`/usr/src/linux/Documentation/initrd.txt`
Manual-Page von `initrd` (`man 4 initrd`).

linuxrc

linuxrc ist ein Programm, das in der Hochlauf-Phase des Kernels gestartet wird, bevor richtig gebootet wird. Diese angenehme Eigenschaft des Kernels erlaubt es, einen kleinen modularisierten Kernel zu booten und die wenigen

Treiber, die man wirklich braucht, als Module nachzuladen– sogar von einer Module-Diskette.

linuxrc hilft bei Bedarf die relevanten Treiber manuell zu laden; im Regelfall kann jedoch heutzutage auf die automatische Hardware-Erkennung vertraut werden, die vor dem Start von YaST2 durchgeführt wird. Sie können linuxrc nicht nur bei der Installation verwenden, sondern auch als Boot-Tool für ein installiertes System und Sie können sogar ein autonomes, RAM-Disk-basiertes Rettungssystem starten, etwa wenn etwas Größeres auf der Festplatte zerstört ist oder wenn Sie schlicht das `root`-Passwort vergessen haben. Näheres finden Sie in Abschnitt *Das SuSE Rettungssystem* auf Seite 212.

Hauptmenü

Nachdem Sprache und Tastatur eingestellt sind, gelangen Sie in das Hauptmenü von linuxrc (vgl. Abbildung 1.2 auf Seite 11). Normalerweise wird linuxrc benutzt, um Linux zu starten; Ziel ist also der Menüpunkt 'Installation / System starten'. Ob Sie direkt zu diesem Punkt gehen können, hängt von der Hardware des Rechners und dem Installationsvorhaben überhaupt ab; Informationen dazu finden Sie in Abschnitt *Textbasierte Installation mit YaST2* auf Seite 8.

Einstellungen

Einstellungen können bezüglich 'Sprache', 'Bildschirm' (Farbe/monochrom), 'Tastaturbelegung' und 'Debug (Experten)' vorgenommen werden.

System-Information

Unter 'System-Information' (Abbildung 10.1 auf der nächsten Seite) können Sie neben den Meldungen des Kernels auch einige weitere Einzelheiten überprüfen, etwa die I/O-Adressen von PCI-Karten oder die Größe des Hauptspeichers, die von Linux erkannt wurde.

Die folgenden Zeilen zeigen, wie sich eine Festplatte und ein CD-ROM-Laufwerk an einem EIDE-Adapter melden. In diesem Fall müssen Sie keine Kernelmodule für eine Installation laden:

```
hda: ST32140A, 2015MB w/128kB Cache, LBA, CHS=1023/64/63
hdb: CD-ROM CDR-S1G, ATAPI CDROM drive
Partition check:
 hda: hda1 hda2 hda3 < hda5 >
```

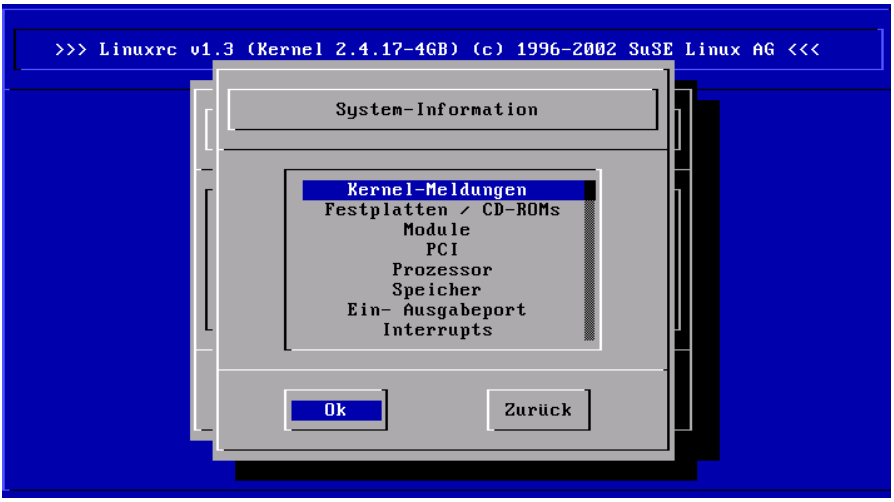


Abbildung 10.1: *Systeminformationen*

Haben Sie einen Kernel gestartet, der bereits einen SCSI-Treiber fest integriert hat, so brauchen Sie natürlich ebenfalls kein SCSI-Modul mehr zu laden. Typische Meldungen bei Erkennung eines SCSI-Adapters und der daran angeschlossenen Geräte:

```
scsi : 1 host.
Started kswapd v 1.4.2.2
scsi0 : target 0 accepting period 100ns offset 8 10.00MHz FAST SCSI-II
scsi0 : setting target 0 to period 100ns offset 8 10.00MHz FAST SCSI-II
  Vendor: QUANTUM   Model: VP32210           Rev: 81H8
  Type:   Direct-Access                      ANSI SCSI revision: 02
Detected scsi disk sda at scsi0, channel 0, id 0, lun 0
scsi0 : target 2 accepting period 236ns offset 8 4.23MHz synchronous SCSI
scsi0 : setting target 2 to period 248ns offset 8 4.03MHz synchronous SCSI
  Vendor: TOSHIBA   Model: CD-ROM XM-3401TA  Rev: 0283
  Type:   CD-ROM                             ANSI SCSI revision: 02
scsi : detected 1 SCSI disk total.
SCSI device sda: hdwr sector= 512 bytes. Sectors= 4308352 [2103 MB] [2.1 GB]
Partition check:
 sda: sda1 sda2 sda3 sda4 < sda5 sda6 sda7 sda8 >
```

Laden von Modulen

Sie wählen aus, welches Modul Sie benötigen. Wurde von der Diskette gebootet, werden nun die entsprechenden Daten von linuxrc eingelesen und im

Folgenden zur Auswahl dargestellt.

Wenn Sie von CD gebootet haben oder von DOS aus mittels loadlin nachgestartet haben, stehen die Module bereits alle linuxrc zur Verfügung. Dies erspart das langwierige Laden, braucht dafür jedoch mehr Speicher.

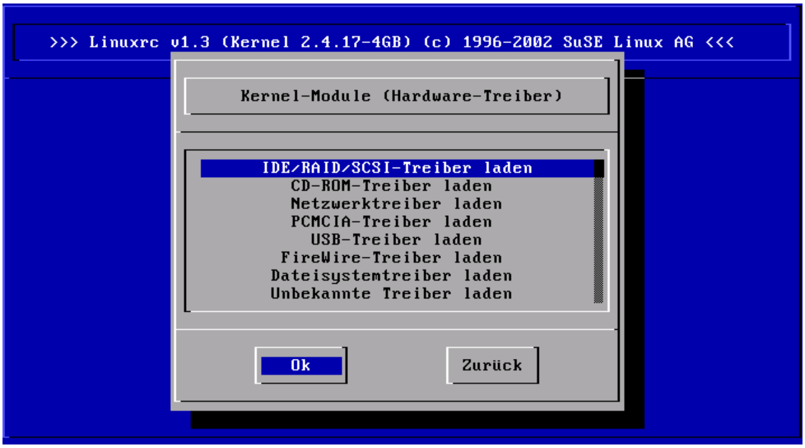


Abbildung 10.2: *Module laden*

linuxrc bietet Ihnen die verfügbaren Treiber in einer Liste an. Links sehen Sie den Namen des zuständigen Moduls, rechts eine Kurzbeschreibung der Hardware, für die der Treiber zuständig ist.

Für einige Komponenten gibt es mitunter mehrere Treiber oder neuere Alpha-Treiber. Auch diese werden hier angeboten.

Parametereingabe

Haben Sie den Treiber gefunden, der für Ihre Hardware zuständig ist, positionieren Sie den Cursor und drücken Sie ⏎. Es erscheint eine Maske, in der Sie etwaige Parameter für das zu ladende Modul eingeben können.

Hier sei noch einmal darauf hingewiesen, dass im Gegensatz zur Parametereingabe am Kernel-Prompt (MILO, LILO oder SYSLINUX) mehrere Parameter für das gleiche Modul durch Leerzeichen voneinander getrennt werden müssen.

In vielen Fällen ist die genaue Spezifizierung der Hardware gar nicht notwendig; die meisten Treiber finden Ihre Komponenten von alleine. Lediglich

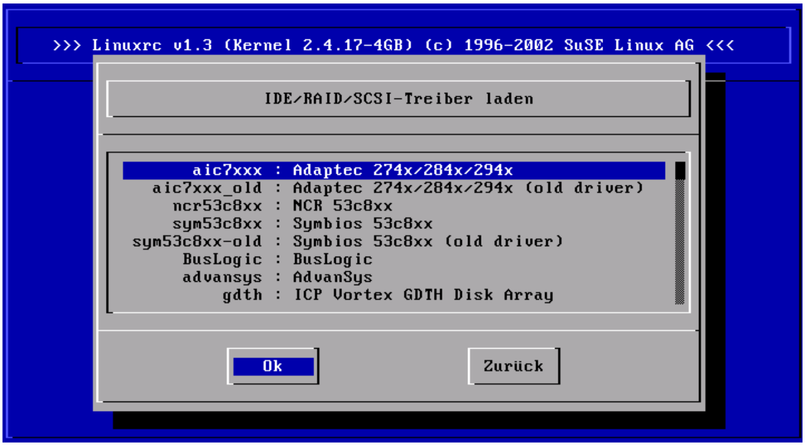


Abbildung 10.3: *Auswahl der SCSI-Treiber*

bei den Netzwerkkarten und bei älteren CD-ROM-Laufwerken mit eigener Controller-Karte ist die Angabe von Parametern mitunter erforderlich. Probieren Sie es jedenfalls erst einmal mit ↵.

Bei einigen Modulen kann das Erkennen und Initialisieren der Hardware recht lange dauern. Durch Umschalten auf die virtuelle Konsole 4 (Alt + F4) können Sie die Meldungen des Kernels während des Ladens beobachten. Vor allem SCSI-Adapter lassen sich etwas Zeit beim Ladevorgang, da sie auch eine gewisse Zeit warten, bis sich alle angeschlossenen Geräte gemeldet haben.

Wurde das Modul erfolgreich geladen, werden die Meldungen des Kernels von linuxrc angezeigt, sodass Sie sich vergewissern können, dass alles wie vorgesehen gelaufen ist. Ansonsten weisen die Meldungen möglicherweise auf die Ursache des Scheiterns hin.

System / Installation starten

Haben Sie die komplette Kernel-Unterstützung für Ihre Hardware erreicht, so können Sie zum Punkt 'System / Installation starten' weitergehen.

Von hier aus (Abbildung 1.3 auf Seite 13) lassen sich mehrere Vorgänge anstoßen: 'Installation/Update starten', 'Installiertes System booten' (die Rootpartition muss bekannt sein), 'Rettungssystem starten' (vgl. Abschnitt *Das SuSE Rettungssystem* auf der nächsten Seite) und 'CD auswerfen'.

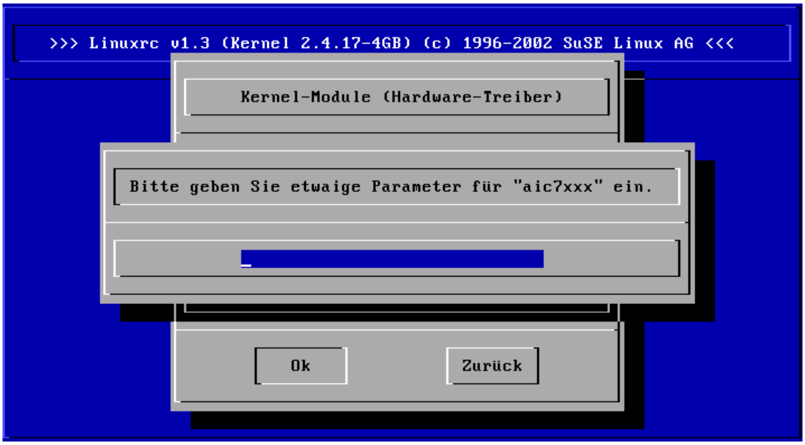


Abbildung 10.4: *Eingabe der Parameter für das Laden eines Moduls*

Der Punkt 'LiveEval-CD starten' steht nur zur Verfügung, wenn Sie von einer „LiveEval-CD" gebootet haben. ISO-Images können vom FTP-Server heruntergeladen werden (`live-eval-`⟨*VERSION*⟩):

`ftp://ftp.suse.com/pub/suse/i386/`

Tipp

Der Punkt 'LiveEval-CD starten' kann z. B. immer dann nützliche Dienste leisten, wenn man *ohne* eigentliche Festplatten-Installation testen möchte, ob der fragliche Rechner oder das anzuschaffende Notebook überhaupt mit SuSE Linux kompatibel ist – ein solcher Test sollte in jedem zeitgemäßen PC-Laden ohne Umstände möglich sein!

Tipp

Für die Installation (Abbildung 10.5 auf der nächsten Seite) und ähnlich auch für das Rettungssystem können Sie verschiedene Quellen wählen (Abbildung 10.6 auf Seite 216).

Das SuSE Rettungssystem

SuSE Linux enthält mehrere Rettungssysteme, mit deren Hilfe Sie in Notfällen „von außen" an Ihre Linux-Partitionen auf den Festplatten kommen können:

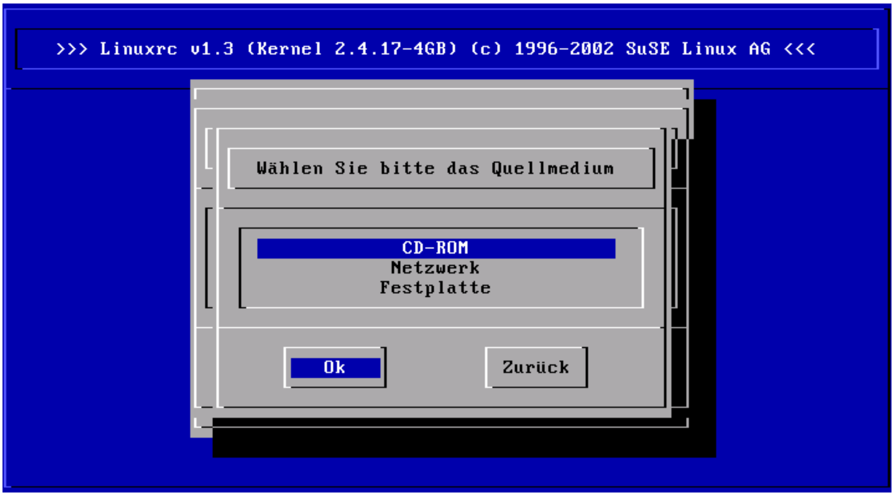


Abbildung 10.5: *Auswahl des Quellmediums in* linuxrc

insbesondere kommen hier die *Bootdiskette* sowie das *„Rescue"–System* in Betracht, das Sie von Diskette, CD, Netzwerk oder vom SuSE-FTP-Server laden können. Weiterhin gibt es eine bootbare SuSE Linux–CD (die *„LiveEval-CD"*), die als Rettungssystem eingesetzt werden kann.

Zum Rettungssystem gehören des Weiteren verschiedene Hilfsprogramme, mit denen Sie Probleme mit unzugänglich gewordenen Festplatten, fehlerhaften Konfigurationsdateien usw. beheben können. Teil des Rettungssystem ist auch Parted (`parted`) zum Verändern der Partitionsgrößen; es kann bei Bedarf aus dem Rettungssystem heraus manuell aufgerufen werden, falls Sie nicht auf den in YaST2 integrierten Resizer zurückgreifen wollen. Informationen zu Parted finden Sie unter:

`http://www.gnu.org/software/parted/`

Tipp

Legen Sie sich immer eine Boot- und Rettungsdiskette an, da der geringe Aufwand für die Erzeugung und Pflege der Disketten in keinem Verhältnis zur Arbeit und dem Zeitverlust steht, wenn Sie im Notfall keinen Zugriff auf Ihr System und auf das CD-ROM-Laufwerk haben.

Tipp

Vorbereitung

Für die Erstellung Ihres Rettungssystems benötigen Sie zwei fehlerfreie Disketten: eine als spätere Bootdiskette, die andere für das komprimierte Abbild eines kleinen Root–Dateisystems. Die Abbilddatei `bootdisk` für das Booten des Systems und die Datei `rescue` für das Root–Dateisystems finden Sie auf der ersten CD unter `boot`.

Es gibt drei Möglichkeiten, um die Diskette mit Root–Dateisystems anzulegen:

- mit YaST
- über eine Konsole mit den Linux–Befehlen

  ```
  erde:~ #  /sbin/badblocks -v /dev/fd0 1440
  erde:~ #  dd if=/media/cdrom/boot/rescue of=/dev/fd0 bs=18k
  ```

- über den DOS-Prompt (wobei `Q:` das CD-ROM-Laufwerk ist)

  ```
  Q:\> cd \dosutils\rawrite
  Q:\dosutils\rawrite> rawrite.exe
  ```

Die Rettungsdiskette basiert z. Z. auf der libc5 (SuSE Linux 5.3), da es in dieser SuSE Linux–Version möglich ist, einige Programme wie z. B. Editor, fdisk oder e2fsck auf einer Diskette unterzubringen.

Hinweis

Die Rettungsdiskette lässt sich nicht mounten, da sie kein Dateisystem, sondern nur das komprimierte Abbild eines solchen enthält. Möchten Sie das Dateisystem einmal einsehen, dann lesen Sie nachfolgenden Absatz.

Hinweis

Wenn Sie in das unkomprimierte Abbild einsehen möchten, müssen Sie die Abbilddatei dekomprimieren und dann das unkomprimierte Abbild als Benutzer `root` mounten. Unterstützt Ihr Linux-Kernel das *loop-Device*, geht der Vorgang wie folgt:

```
erde:~ #  cp /media/cdrom/boot/rescue /root/rescue.gz
erde:~ #  gunzip /root/rescue.gz
erde:~ #  mount -t ext2 -o loop /root/rescue /mnt
```

Das Rettungssystem starten

Das Rettungssystem wird von der selbsterstellten SuSE-Bootdiskette bzw. der bootbaren CD oder der DVD gestartet. Die Voraussetzung ist, dass das Disketten- bzw. CD-ROM/DVD-Laufwerk bootfähig ist; nötigenfalls müssen Sie im CMOS-Setup die Boot-Reihenfolge ändern.

Nachfolgend die Schritte zum Starten des Rettungssystems:

1. Legen Sie die selbsterstellte SuSE-Bootdiskette (`bootdisk`) bzw. die erste CD oder DVD von SuSE Linux in das entsprechende Laufwerk ein und schalten Sie Ihr System ein.

2. Sie können entweder das System durchbooten lassen oder Sie wählen 'Manual Installation' aus und können dann – falls notwendig – bei den 'boot options' Parameter angeben. Im Folgenden ist es möglich festzulegen, welche Kernel-Module geladen werden sollen.

3. Nehmen Sie im linuxrc die erforderlichen Einstellungen für die Sprache und die Tastatur vor.

4. Wählen Sie im Hauptmenü den Punkt 'Installation/System starten'.

5. Wenn Sie mit der *Bootdiskette* gestartet haben, legen Sie nun die InstallationsCD oder die Diskette (`rescue`) mit dem komprimierten Abbild des Rettungssystems ein.

6. Wählen Sie im Menü 'Installation/System starten' den Punkt 'Rettungssystem starten' (s. Abb. 1.3 auf Seite 13) und geben Sie dann das gewünschte Quellmedium an (s. Abb. 10.6 auf der nächsten Seite).

   Im Anschluss ein paar Hinweise zu den Auswahlmöglichkeiten:

   'CD-ROM' Beim Laden des Rettungssystems wird der Pfad `/cdrom` exportiert. Eine Installation ist so von *dieser* CD aus möglich.

   'Netzwerk' Um das `rescue`-System über eine Netzverbindung zu starten; der Treiber für die Netzwerkkarte muss zuvor geladen worden sein; vgl. die allgemeinen Hinweise in Abschnitt *Installation von einer Quelle im „Netz"* auf Seite 18. In einem Untermenü stehen mehrere Protokolle zur Verfügung (s. Abb. 10.7 auf Seite 217): NFS, FTP, SMB etc.

   'Festplatte' Laden Sie das `rescue`-System von der Festplatte aus.

   'Diskette' Das `rescue`-System kann auch von Diskette gestartet werden, vor allem wenn der Rechner über wenig Arbeitsspeicher verfügt.

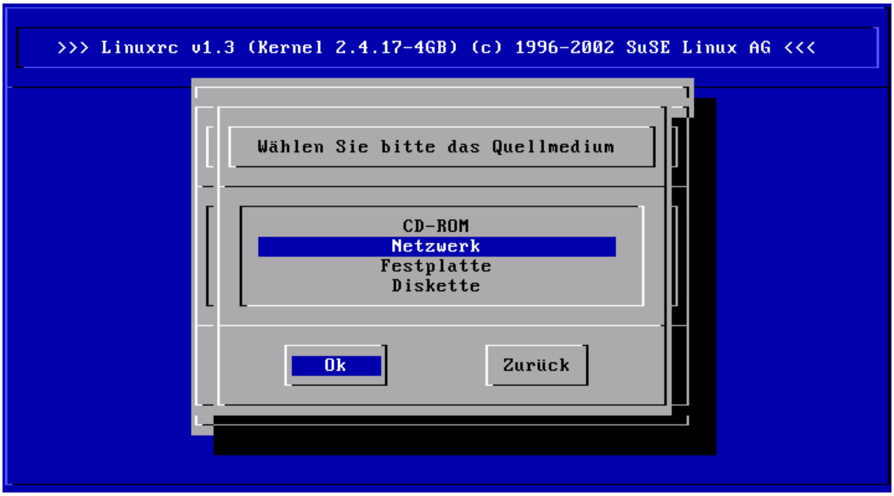


Abbildung 10.6: *Quellmedium für das rescue-System*

Welches Medium Sie auch gewählt haben, das Rettungssystem wird dekomprimiert und als neues Root-Dateisystem in eine RAM-Disk geladen, gemountet und gestartet. Es ist damit betriebsbereit.

Das Rettungssystem benutzen

Das Rettungssystem stellt Ihnen unter Alt + F1 bis Alt + F3 mindestens drei virtuelle Konsolen zur Verfügung, an denen Sie sich als Benutzer `root` ohne Passwort einloggen können. Mit Alt + F10 kommen Sie zur Systemkonsole mit den Meldungen von Kernel und syslog.

In dem Verzeichnis `/bin` finden Sie die Shell und Utilities (z. B. mount). Wichtige Datei- und Netz-Utilities, z. B. zum Überprüfen und Reparieren von Dateisystemen (e2fsck), liegen im Verzeichnis `/sbin`. Des Weiteren finden Sie in diesem Verzeichnis auch die wichtigsten Binaries für die Systemverwaltung wie fdisk, mkfs, mkswap, init, shutdown, sowie für den Netzwerkbetrieb ifconfig, route und netstat.

Als Editor ist der vi unter `/usr/bin` verfügbar; hier sind auch weitere Tools (grep, find, less etc.) wie auch das Programm telnet zu finden.

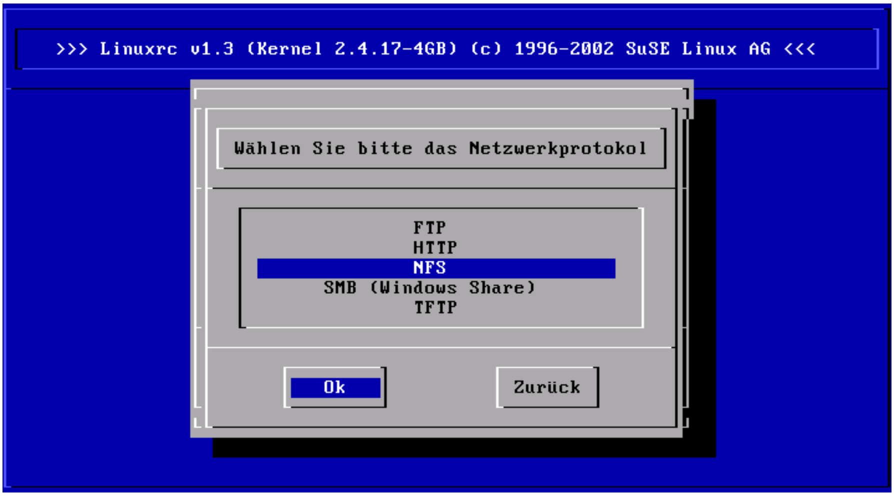


Abbildung 10.7: *Netzwerkprotokolle*

Zugriff auf das normale System

Zum Mounten Ihres SuSE Linux-Systems auf der Platte ist der Mountpoint `/mnt` gedacht. Sie können für eigene Zwecke weitere Verzeichnisse erzeugen und als Mountpoints verwenden.

Nehmen wir als Beispiel einmal an, Ihr normales System setzt sich laut `/etc/fstab` wie in der Beispieldatei 14 beschrieben zusammen.

```
/dev/sdb5       swap         swap         defaults    0   0
/dev/sdb3       /            ext2         defaults    1   1
/dev/sdb6       /usr         ext2         defaults    1   2
```

Datei 14: *Beispiel /etc/fstab*

Achtung

Beachten Sie im folgendem Abschnitt die Reihenfolge, in welcher die einzelnen Geräte zu mounten sind.

Achtung

Um Zugriff auf Ihr gesamtes System zu haben, mounten Sie es Schritt für Schritt unter `/mnt` mit den folgenden Befehlen:

```
erde:/ #  mount /dev/sdb3 /mnt
```

```
erde:/ #  mount /dev/sdb6 /mnt/usr
```

Nun haben Sie Zugriff auf Ihr ganzes System und können z. B. Fehler in Konfigurationsdateien wie `/etc/fstab`, `/etc/passwd`, `/etc/inittab` beheben. Die Konfigurationsdateien befinden sich statt im Verzeichnis `/etc` jetzt im Verzeichnis `/mnt/etc`.

Um selbst komplett verloren gegangene Partitionen mit dem Programm fdisk einfach wieder durch Neu-Anlegen zurückzugewinnen – wenn bekannt war, wo die Partitionen vorher auf der Festplatte lagen – sollten Sie sich einen Ausdruck (Hardcopy) von dem Verzeichnis `/etc/fstab` und dem Output des Befehls

```
erde:~ #  fdisk -l /dev/⟨disk⟩
```

machen. Anstelle der Variablen ⟨*disk*⟩ setzen Sie bitte der Reihe nach die Gerätenamen (engl. *devices*) Ihrer Festplatten ein, z. B. `hda`.

Dateisysteme reparieren

Beschädigte Dateisysteme sind ein besonders ernster Anlass für den Griff zum Rettungssystem. Dies kann z. B. nach einem unsauberen Shutdown (wie bei Stromausfall) oder einem Systemabsturz vorkommen. Dateisysteme lassen sich grundsätzlich nicht im laufenden Betrieb reparieren. Bei schwereren Schäden lässt sich unter Umständen nicht einmal das Root-Dateisystem mehr mounten und der Systemstart endet in einer "kernel panic". Da bleibt nur der Weg, die Reparatur „von außen“ unter einem Rettungssystem zu versuchen.

Im SuSE Linux-Rettungssystem sind die Utilities e2fsck und dumpe2fs (zur Diagnose) enthalten. Damit beheben Sie die meisten Probleme. Und da auch im Notfall oft die Manual-Page von e2fsck nicht mehr zugänglich ist, ist sie im Anhang B auf Seite 381 ausgedruckt.

Beispiel: Wenn sich ein Dateisystem wegen eines *ungültigen Superblocks* nicht mehr mounten lässt, wird das Programm e2fsck vermutlich zunächst ebenfalls scheitern. Die Lösung ist, die im Dateisystem alle 8192 Blöcke (8193, 16385...) angelegt und gepflegten Superblock-Backups zu verwenden. Dies leistet z. B. der Befehl:

```
erde:~ #  e2fsck -f -b 8193 /dev/⟨Defekte_Partition⟩
```

Die Option `-f` erzwingt den Dateisystem-Check und kommt damit dem möglichen Irrtum von `e2fsck` zuvor, es sei – angesichts der intakten Superblock-Kopie – alles in Ordnung.

Virtuelle Konsolen

Linux ist multitasking- und multiuserfähig. Auch bei einem Ein-Benutzer-PC--System werden Sie die Vorteile, die diese Fähigkeiten mitbringen, schätzen lernen:

Im Textmodus stehen 6 virtuelle Konsolen zur Verfügung, zwischen denen Sie durch die Tastenkombinationen Alt + F1 bis Alt + F6 wechseln können. Die siebte Konsole ist für X11 reserviert. Durch Modifikation der Datei `/etc/inittab` können auch weitere oder weniger Konsolen zur Verfügung gestellt werden.

Wenn Sie von X11 aus auf eine Textkonsole zurückschalten möchten, ohne X11 zu beenden, verwenden Sie Ctrl + Alt + F1 bis Ctrl + Alt + F6. Mit Alt + F7 kommen Sie zu X11 zurück.

Tastaturbelegung

Um die Tastaturbelegung von Programmen zu vereinheitlichen, wurden Änderungen an den folgenden Dateien vorgenommen:

```
/etc/inputrc
/usr/X11R6/lib/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/X11R6/lib/X11/app-defaults/XTerm
/usr/share/emacs/⟨VERSION⟩/site-lisp/term/*.el
/usr/lib/joerc
```

Diese Änderungen wirken sich nur auf die Applikationen aus, die die `terminfo`-Einträge auslesen, bzw. deren Konfigurationsdateien direkt verändert wurden (`vi`, `less` etc.). Andere nicht-SuSE-Applikationen sollten an diese Vorgaben angepasst werden.

Unter X ist die Compose-Taste („Multi_key“) über die Tastenkombination Ctrl + ⇑ (rechts) zu erreichen; vgl. den Eintrag in `/usr/X11R6/lib/X11/Xmodmap`.

Lokale Anpassungen – I18N/L10N

SuSE Linux ist sehr weitgehend internationalisiert und kann flexibel auf lokale Gegebenheiten abgestimmt werden; anders gesagt: die Internationalisierung („I18N“) erlaubt spezielle Lokalisierungen („L10N“). Die Abkürzungen I18N und L10N stehen für *internationalization* und *localization*: jeweils Anfangs- und Endbuchstabe und dazwischen die Anzahl der ausgelassenen Buchstaben.

Die Einstellungen werden über `LC_*`-Variablen vorgenommen, die in der Datei `/etc/sysconfig/language` definiert sind. Dabei geht es nicht nur um die Einstellung der Sprache für die Programmoberfläche und -meldungen (engl. *native language support*), sondern im Einzelnen um die Kategorien für *Nachrichten* (Sprache), *Zeichenklassen*, *Sortierreihenfolge*, *Datum und Uhrzeit*, *Zahlen* und *Geld*. Jede dieser Kategorien kann entweder gezielt über eine eigene Variable oder indirekt über eine übergeordnete Variable in der Datei `language` festgelegt werden (vgl. Manual-Page von `locale` (`man 5 locale`)):

1. `RC_LC_MESSAGES`, `RC_LC_CTYPE`, `RC_LC_COLLATE`, `RC_LC_TIME`, `RC_LC_NUMERIC`, `RC_LC_MONETARY`: Diese Variablen werden ohne den `RC_`-Vorsatz an die Shell weitergereicht und bestimmen die o. g. Kategorien; die betroffenen Dateien werden im Folgenden aufgezählt.

   Die aktuelle Einstellung kann mit dem Befehl `locale` abgefragt werden.

2. `RC_LC_ALL`: Diese Variable überschreibt, falls gesetzt, die Werte der in Punkt 1 genannten Variablen.

3. `RC_LANG`: Wenn keine der o. g. Variablen gesetzt ist, ist diese der „Fallback“. SuSE Linux setzt standardmäßig nur `RC_LANG`; dadurch kann der Anwender leichter eigene Werte eintragen.

4. `ROOT_USES_LANG`: Eine `yes`/`no`-Variable. Ist sie auf `no` gesetzt, dann arbeitet `root` immer in der POSIX-Umgebung.

Die Variablen sind über den `sysconfig`-Editor zu setzen.

Der Wert einer solchen Variablen setzt sich aus Sprachangabe (engl. *language code*), Land oder Territorium (engl. *country code*), Zeichensatz (engl. *encoding*) und Option (engl. *modifier*) zusammen. Die einzelnen Angaben werden mit Spezialzeichen verbunden:

LANG=⟨*language*⟩[[_⟨*COUNTRY*⟩].Encoding[@Modifier]]

Einige Beispiele

Bitte setzen Sie die Sprach- und die Länderangabe immer zusammen. Die Angabe der Sprache folgt dem Standard ISO 639 (http://www.evertype.com/standards/iso639/iso639-en.html und http://www.loc.gov/standards/iso639-2/), die Ländercodes sind in ISO 3166 (http://www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html) festgelegt. Sinnvollerweise dürfen aber nur die Werte gewählt werden, für die verwendbare Beschreibungsdateien unter `/usr/lib/locale` zu finden sind. Weitere Beschreibungsdateien lassen sich mit Hilfe von `localedef` aus den Dateien in `/usr/share/i18n` erzeugen. Eine Beschreibungsdatei für `de_DE@euro.UTF-8` wird so erzeugt mit:

```
erde:~ #  localedef -i de_DE@euro -f UTF-8 de_DE@euro.UTF-8
```

LANG=de_DE.ISO-8859-1

So stellt man deutsche Sprache in Deutschland mit Zeichensatz `ISO-8859-1` ein. Dieser Zeichensatz enthält nicht das Euro-Zeichen; man benötigt diesen Zeichensatz bisweilen noch, wenn ein Programm noch nicht an `ISO-8859-15` angepasst ist.

Die Angabe des Zeichensatzes (hier `ISO-8859-1`) wertet z. B. der Emacs aus.

LANG=de_DE@euro

Dies ist ein Beispiel für das Setzen einer Option (`euro`). Die Einstellung `de_DE@euro` ist die Vorgabe für eine Standardinstallation in deutscher Sprache.

LANG=de_DE.UTF-8

Wenn man in einem Unicode-xterm arbeitet, ist die Angabe `UTF-8` zu machen. Um ein xterm für UTF-8 zu starten, sollte man sich ein einfaches Shell-Skript etwa unter dem Namen `uxterm` anlegen; vgl. Datei 15.

```
#!/bin/bash
export LANG=de_DE.UTF-8
xterm -fn \
 -Misc-Fixed-Medium-R-Normal--18-120-100-100-C-90-ISO10646-1 \
 -T 'xterm UTF-8' $*
```

Datei 15: *uxterm zum Starten eines Unicode-xterm*

SuSEconfig liest die Variablen aus `/etc/sysconfig/language` aus und schreibt die Angaben nach `/etc/SuSEconfig/profile` und `/etc/SuSEconfig/csh.cshrc`. `/etc/SuSEconfig/profile` wird von `/etc/profile` eingelesen („gesourcet") und `/etc/SuSEconfig/csh.cshrc` von `/etc/csh.cshrc`. Somit stehen die Einstellungen systemweit zur Verfügung.

Die Benutzer können die Systemvorgaben in `~/.bashrc` überschreiben. Wenn also die Systemvorgabe `de_DE` ist, kann der Benutzer, falls er mit deutschen Programmmeldungen nicht zufrieden ist, so auf englische Ausgaben umschalten:

```
LC_MESSAGES=en_US
```

Anpassung für Sprachunterstützung

Hinweisend ist zu sagen, dass die Dateien der Kategorie *Nachrichten* in der Regel nur im Sprachverzeichnis (z. B. `de`) abgelegt werden, um ein Fallback zu haben. Wenn man also `LANG` auf `de_AT` setzt und die „Message"-Datei unter `/usr/share/locale/de_AT/LC_MESSAGES` nicht vorhanden ist, dann wird auf `/usr/share/locale/de/LC_MESSAGES` zurückgegriffen.

Auch kann man mit `LANGUAGE` eine Fallbackkaskade festlegen; z. B. für bretonisch → französisch oder für galizisch → spanisch → portugiesisch:

```
LANGUAGE="br_FR:fr_FR"
LANGUAGE="gl_ES:es_ES:pt_PT"
```

Oder um – je nach Vorliebe – auf die norwegischen Variaten „nynorsk" bzw. „bokmål" auszuweichen (mit zusätzlichem Rückfall auf `no`):

```
LANG="nn_NO"
LANGUAGE="nn_NO:nb_NO:no"
```

oder

```
LANG="nb_NO"
LANGUAGE="nb_NO:nn_NO:no"
```

Bei Norgwegisch ist auch zu beachten, dass `LC_TIME` unterschiedlich behandelt wird.

Mögliche Probleme

- Der Tausenderpunkt wird nicht erkannt. Wahrscheinlich steht LANG beispielweise auf de. Da die Beschreibung, auf die die glibc zurückgreift, in /usr/share/locale/de_DE/LC_NUMERIC zu finden ist, muss beispielsweise LC_NUMERIC auf de_DE gesetzt werden.

Weitere Informationen:

- *The GNU C Library Reference Manual*, Kap. "Locales and Internationalization"; enthalten im Paket glibc-info.
- Jochen Hein [Hei96], unter dem Stichwort "NLS".
- *German-Howto* von Winfried Trümper file:/usr/share/doc/howto/en/html/German-HOWTO.html
- Markus Kuhn, *UTF-8 and Unicode FAQ for Unix/Linux*, aktuell unter http://www.cl.cam.ac.uk/~mgk25/unicode.html.
- *Unicode-Howto* von Bruno Haible file:/usr/share/doc/howto/en/html/Unicode-HOWTO.html.

Das Bootkonzept

Das Booten und die Initialisierung eines Unix-Systems sind selbst für einem erfahrenen System-Administrator keineswegs trivial. Dieses Kapitel gibt eine kurze Einführung in das Bootkonzept von SuSE Linux. Die vorliegende Implementierung setzt den Abschnitt *System Initialization* der LSB-Spezifikation (Version 1.2) um; zum LSB vgl. Abschnitt *Linux Standard Base (LSB)* auf Seite 196.

Das init-Programm 226
Die Runlevels 226
Wechsel des Runlevels 228
Die Init-Skripten 229
Der YaST2 Runlevel-Editor 232
SuSEconfig, /etc/sysconfig und /etc/rc.config 233
Systemkonfiguration mit dem YaST2 Sysconfig-Editor . . . 235
Skripte und Variablen – Konfiguration des Systems 235

Mit den lapidaren Worten "Uncompressing Linux..." übernimmt der Kernel die Kontrolle über die gesamte Hardware des Systems. Er prüft und setzt die Konsole – oder genauer: die BIOS-Register der Graphikkarte und das Ausgabeformat auf den Bildschirm –, um danach die Einstellungen im BIOS zu lesen und die elementaren Schnittstellen des Mainboards zu initialisieren.
In den nächsten Schritten „proben“ die einzelnen Treiber – die ja Bestandteil des Kernels sind – die vorhandene Hardware, um sie gegebenenfalls zu initialisieren. Nach dem Überprüfen der Partitionen und dem Mounten des Root-Dateisystems startet der Kernel das Programm init. Durch init wird das eigentliche System „hochgefahren“ (Unix-Jargon) und die vielen Dienstprogramme und deren Konfiguration werden so gestartet. Der Kernel verwaltet dann das gesamte System; er überwacht Rechenzeit für die einzelnen Programme, er stellt Speicher zur Verfügung und steuert Hardware-Zugriffe.

Das init-Programm

Das Programm init ist der für die korrekte Initialisierung des Systems zuständige Prozess; es ist sozusagen der „Vater aller Prozesse“ im System.

Unter allen Programmen nimmt init eine Sonderrolle ein: init wird direkt vom Kernel gestartet und ist immun gegen das Signal 9, mit dem normalerweise jeder Prozess „gekillt“ werden kann. Alle weiteren Prozesse werden entweder von init selbst oder von einem seiner „Kindprozesse“ gestartet.

Konfiguriert wird init zentral über die Datei `/etc/inittab`; hier werden die so genannten „Runlevels“ definiert (mehr dazu im nächsten Abschnitt *Die Runlevels* auf dieser Seite) und es wird festgelegt, welche Dienste und Daemonen in den einzelnen Levels zur Verfügung stehen sollen. Abhängig von den Einträgen in `/etc/inittab` ruft init verschiedene Skripten auf, die aus Gründen der Übersichtlichkeit im Verzeichnis `/etc/init.d` zusammengefasst sind.

Der gesamte Hochlauf des Systems – und natürlich auch das Herunterfahren – wird somit einzig und allein vom init-Prozess gesteuert; insofern lässt sich der Kernel quasi als „Hintergrundprozess“ betrachten, dessen Aufgabe darin besteht, die gestarteten Prozesse zu verwalten, ihnen Rechenzeit zuzuteilen und den Zugriff auf die Hardware zu ermöglichen und zu kontrollieren.

Die Runlevels

Unter Linux existieren verschiedene *Runlevels*, die den jeweiligen Zustand des Systems definieren. Der Standard-Runlevel, in dem das System beim Booten

hochfährt, ist in der Datei /etc/inittab durch den Eintrag initdefault festgelegt. Für gewöhnlich ist dies 3 oder 5 (siehe Tabelle 11.1 auf der nächsten Seite). Alternativ kann der gewünschte Runlevel beim Booten (z. B. am Boot-Prompt) angegeben werden; der Kernel reicht die Parameter, die er nicht selbst auswertet, unverändert an den init-Prozess weiter.

Um zu einem späteren Zeitpunkt in einen anderen Runlevel zu wechseln, kann man init mit der Nummer des zugehörigen Runlevels aufrufen; das Wechseln des Runlevels kann nur vom Systemadministrator veranlasst werden.

Beispielsweise gelangt man durch das Kommando

```
root@erde:/ >  init 1
```

in den *Einzelbenutzerbetrieb* (engl. *Single user mode*), der der Pflege und Administration des Systems dient. Nachdem der Systemadministrator seine Arbeit beendet hat, kann er durch

```
root@erde:/ >  init 3
```

das System wieder in den normalen Runlevel hochfahren lassen, in dem alle für den Betrieb erforderlichen Programme laufen und sich die einzelnen Benutzer beim System anmelden können.

Die Tabelle 11.1 auf der nächsten Seite gibt einen Überblick über die zur Verfügung stehenden Runlevel. Runlevel 2 sollte auf einem System, dessen /usr-Partition via NFS gemountet ist, nicht verwendet werden!

Daraus folgt insbesondere, dass Sie das System auch durch

```
root@erde:/ >  init 0
```

anhalten, bzw. durch

```
root@erde:/ >  init 6
```

zu einem Neustart veranlassen können.

Bei einer Standardinstallation von SuSE Linux wird normalerweise Runlevel 5 als Standard eingerichtet, so dass sich die Benutzer direkt an der grafischen Oberfläche beim System anmelden können. Sollte die Einrichtung von Runlevel 5 durch manuellen Eingriff verhindert worden sein, so kann man nun nachträglich eine Umkonfiguration vornehmen.

Wenn Sie den Runlevel von 3 auf 5 setzen wollen, muss sichergestellt sein, dass das X Window System bereits korrekt konfiguriert ist; (Kapitel ?? auf Seite ??). Ob das System so wie von Ihnen gewünscht funktioniert, testen Sie danach durch Eingabe von:

Runlevel	Bedeutung
0	Systemhalt (engl. *System halt*)
S	Einzelbenutzerbetrieb (engl. *Single user mode*); vom Bootprompt aus mit US-Tastaturbelegung
1	Einzelbenutzerbetrieb (engl. *Single user mode*)
2	Lokaler Multiuserbetrieb ohne entferntes Netzwerk (engl. *Local multiuser without remote network (e. g. NFS)*)
3	Voller Multiuserbetrieb mit Netzwerk (engl. *Full multiuser with network*)
4	Frei (engl. *Not used*)
5	Voller Multiuserbetrieb mit Netzwerk und KDM (Standard), GDM oder XDM (engl. *Full multiuser with network and xdm*)
6	Systemneustart (engl. *System reboot*)

Tabelle 11.1: *Liste der gültigen Runlevels unter Linux*

```
root@erde:/ > init 5
```

Ist dies der Fall, können Sie den Standard-Runlevel über YaST2 auf `5` ändern.

Achtung

Eigene Änderungen an `/etc/inittab`

Eine fehlerhafte `/etc/inittab` kann dazu führen, dass das System nicht korrekt hochgefahren wird. Gehen Sie bei Veränderungen dieser Datei mit äusserster Sorgfalt vor und behalten Sie immer eine Kopie einer intakten Datei. Zur Behebung des Schadens können Sie versuchen, am LILO-Prompt den Parameter `init=/bin/sh` zu übergeben, um direkt in eine Shell zu booten und von dort aus die Datei wiederherzustellen. Nach dem Booten spielen Sie mittels `cp` die Backupkopie wieder ein.

Achtung

Wechsel des Runlevels

Generell passieren bei einem Wechsel des Runlevels folgende Dinge: Die *Stopp-Skripten* des gegenwärtigen Runlevels werden ausgeführt – dabei werden typischerweise verschiedene, in diesem Level laufende Programme beendet – und die *Start-Skripten* des neuen Runlevels werden ausgeführt. Wäh-

rend eines solchen Vorgangs werden in den meisten Fällen einige Programme gestartet.

Um dies zu verdeutlichen, betrachten wir an einem Beispiel den Wechsel von Runlevel 3 nach Runlevel 5:

- Der Administrator (`root`) teilt dem init-Prozess mit, dass der Runlevel gewechselt werden soll:

  ```
  root@erde:/ >  init 5
  ```

- init konsultiert die Konfigurationsdatei `/etc/inittab` und stellt fest, dass das Skript `/etc/init.d/rc` mit dem neuen Runlevel als Parameter aufgerufen werden muss.
- Nun ruft rc alle Stopp-Skripten des gegenwärtigen Runlevels auf, für die im neuen Runlevel kein Start-Skript existiert; in unserem Beispiel sind das alle Skripte, die sich im Verzeichnis `/etc/init.d/rc3.d` befinden (der alte Runlevel war `3`) und mit einem `'K'` beginnen. Die nach dem `'K'` folgende Zahl gewährleistet, dass hierbei eine bestimmte Reihenfolge eingehalten wird, da unter Umständen manche Programme von anderen abhängig sind.

  Hinweis

  Die Namen der Stopp-Skripten beginnen immer mit `'K'` (engl. *kill*), die der Start-Skripten mit `'S'` (engl. *start*).

  Hinweis

- Als Letztes werden die Start-Skripten des neuen Runlevels aufgerufen; diese liegen in unserem Beispiel unter `/etc/init.d/rc5.d` und beginnen mit einem `'S'`. Auch hierbei wird eine bestimmte Reihenfolge eingehalten, die durch die dem `'S'` folgende Zahl festgelegt ist.

Wenn Sie in denselben Runlevel wechseln, in dem Sie sich bereits befinden, liest init nur die `/etc/inittab` ein, prüft sie auf Veränderungen und nimmt bei Bedarf die entsprechenden Maßnahmen vor, etwa das Starten eines `getty` auf einer weiteren Schnittstelle.

Die Init-Skripten

Die Skripten unter `/etc/init.d` unterteilen sich in zwei Kategorien:

Option	Bedeutung
`start`	Dienst starten
`stop`	Dienst stoppen
`restart`	Dienst stoppen und erneut starten, wenn der Dienst bereits lief; andernfalls den Dienst starten
`reload`	Konfiguration des Dienstes erneut einlesen, ohne den Dienst zu stoppen und neu zu starten
`force-reload`	Konfiguration des Dienstes erneut einlesen, wenn der Dienst dies unterstützt; andernfalls wie `restart`
`status`	aktuellen Status anzeigen

Tabelle 11.2: *Übersicht der Optionen der init-Skripten*

- Skripte, die direkt von init aufgerufen werden: Dies ist nur beim Booten der Fall sowie bei einem sofortigen Herunterfahren des Systems (bei Stromausfall oder durch Drücken der Tastenkombination Ctrl + Alt + Entf durch den Anwender).
- Skripte, die indirekt von init aufgerufen werden: Das geschieht bei einem Wechsel des Runlevels; es wird generell das übergeordnete Skript /etc/init.d/rc ausgeführt, das dafür sorgt, dass die relevanten Skripten in der korrekten Reihenfolge aufgerufen werden.

Alle Skripten befinden sich unter `/etc/init.d`. Die Skripten für das Wechseln des Runlevels befinden sich ebenfalls in diesem Verzeichnis, werden jedoch grundsätzlich als symbolischer Link aus einem der Unterverzeichnisse `/etc/init.d/rc0.d` bis `/etc/init.d/rc6.d` aufgerufen. Dies dient der Übersichtlichkeit und vermeidet, dass Skripten mehrfach vorhanden sein müssen, etwa weil sie in verschiedenen Runlevels verwendet werden sollen. Da jedes dieser Skripten sowohl als Start- wie auch als Stopp-Skript aufgerufen werden kann, müssen sie alle die beiden möglichen Parameter `start` und `stop` verstehen. Zusätzlich verstehen die Skripten die Optionen `restart`, `reload`, `force-reload` und `status`; die Bedeutung aller Optionen ist in Tabelle 11.2 aufgelistet.

Beim Verlassen des Runlevels 3 wird `/etc/init.d/rc3.d/K40network` aufgerufen; `/etc/init.d/rc` ruft das Skript `/etc/init.d/network` mit dem Parameter `stop` auf. Beim Eintritt in Runlevel 5 wird letztlich das gleiche Skript gestartet, diesmal jedoch mit dem Parameter `start`.

Die Links in den einzelnen Runlevel-spezifischen Unterverzeichnissen dienen somit also nur dazu, eine Zuordnung der einzelnen Skripten zu bestimmten

Runlevels zu ermöglichen.

Die Anlage und das Entfernen der notwendigen Links geschieht mit insserv (bzw. dem Link `/usr/lib/lsb/install_initd`) beim Installieren oder Deinstallieren des jeweiligen Paketes; vgl. Manual-Page von `insserv` (`man 8 insserv`).

Im Folgenden finden Sie eine kurze Beschreibung der ersten Boot- und der letzten Shutdown-Skripten sowie des Steuerskripts:

boot Wird beim Start des Systems ausgeführt und direkt von init gestartet. Es ist unabhängig vom gewünschten Default-Runlevel und wird nur genau ein einziges Mal ausgeführt: Im Wesentlichen werden `proc`- und `devpts`-Dateisystem eingehängt („gemountet"), der blogd (engl. *Boot Logging Daemon*) wird aktiert und – nach einer Erstinstallation oder einem Update des Systems – wird eine Grundkonfiguration angestoßen.

Diesem Skript ist des Weiteren das Verzeichnis `/etc/init.d/boot.d` zugeordnet; alle in diesem Verzeichnis gefundenen Skripte, die mit `'S'` beginnen, werden automatisch beim Hochlauf des Systems ausgeführt. Es werden die Dateisysteme geprüft, etwaige überflüssige Dateien unter `/var/lock` gelöscht und das Netzwerk für das Loopback-Device konfiguriert, sofern dies vorgesehen ist. Weiterhin wird die Systemzeit gesetzt.

Tritt beim Prüfen und automatischen Reparieren der Dateisysteme ein schwerer Fehler auf, hat der Systemadministrator nach Eingabe des Root-Passwortes die Möglichkeit, manuell eine Lösung des Problems herbeizuführen.

Schließlich wird das Skript boot.local ausgeführt.

boot.local Hier können weitere Dinge eingetragen werden, die beim Start geschehen sollen, bevor das System in einen der Runlevels eintritt; es kann von seiner Funktion her mit der vielleicht von DOS her gewohnten `AUTOEXEC.BAT` verglichen werden.

boot.setup Grundlegende Einstellungen, die beim Übergang vom Einzelnutzerbetrieb in irgendeinen Runlevel vorgenommen werden müssen.

Hier werden die Tastaturbelegung und die Konsolenkonfiguration geladen.

halt Dieses Skript wird nur beim Eintritt in den Runlevel 0 oder 6 ausgeführt. Dabei wird es entweder unter dem Namen `halt` oder dem Namen `reboot` aufgerufen. Abhängig davon, wie halt aufgerufen wurde, wird das System neu gestartet oder ganz heruntergefahren.

rc Das übergeordnete Skript, das bei jedem Wechsel des Runlevels aufgerufen wird. Es führt die Stopp-Skripten des gegenwärtigen Runlevels aus und danach die Start-Skripten des neuen.

Eigene Skripten lassen sich anhand dieses Konzepts hinzufügen. Ein Gerüst ist in `/etc/init.d/skeleton` vorbereitet. Das genaue Format ist im Entwurf des LSB beschrieben; dort wird insbesondere festgelegt, in welcher Reihenfolge und in welchen Levels das jeweilige Skript abgearbeitet werden muss. Nun sind Links mit `insserv` von dem jeweiligen `rc`-Verzeichnis auf das neue Skript anzulegen, damit das Skript – wie oben beschrieben – beim Wechsel des Runlevels ausgeführt wird; die Namengebung für die Links wird ebendort beleuchtet. Die technischen Details werden in der Manual-Page von `init.d` (`man 7 init.d`) und Manual-Page von `insserv` (`man 8 insserv`) dargestellt. Als grafisches Konfigurationswerkzeug zum Anlegen der Links steht der Runlevel-Editor von YaST2 zur Verfügung; vgl. Abschnitt *Der YaST2 Runlevel-Editor* auf dieser Seite.

Achtung

Erstellung eigener init-Skripten
Fehlerhafte init-Skripten können das gesamte System „aufhängen“. Erstellen Sie eigene Skripte mit äusserster Sorgfalt und testen Sie sie – soweit möglich – vor dem Ernstfall in der Multiuserumgebung. Grundlageninformation zum Umgang mit Runleveln/init-Skripten finden Sie im Abschnitt *Die Runlevels* auf Seite 226.

Achtung

Der YaST2 Runlevel-Editor

Nach dem Start wird dieses Experten-Modul zunächst initialisiert. Im nächsten Dialog wird der aktuelle Standard-Runlevel angezeigt. Dieser „Betriebsmodus“ wird nach dem Booten Ihres Systems hochgefahren. Bei SuSE Linux ist dies üblicherweise Runlevel 5 (voller Multiuserbetrieb mit Netzwerk und KDM, dem grafischen Login). Geeignet wäre z. B. auch Runlevel 3 (voller Multiuserbetrieb mit Netzwerk). An dieser Stelle lässt sich mit Hilfe von YaST2 ein anderer Default-Runlevel einstellen; vgl. Tabelle 11.1 auf Seite 228.

Mit ‘Bearbeiten’ gelangen Sie zu einer Übersicht aller Dienste und Daemonen mit der Information, ob diese in Ihrem System aktiv geschaltet sind und für welche Runlevels dies gilt. Wenn Sie eine Zeile per Mausklick markieren, haben Sie die Möglichkeit, die Checkboxen für die Runlevels ‘0’, ‘1’, ‘2’, ‘3’,

'5', '6' und 'S' zu aktivieren und damit festzulegen, für welche Runlevels der entsprechende Dienst bzw. Daemon aktiv werden soll. Runlevel 4 ist nicht definiert – dieser ist stets frei für benutzereigene Einstellungen.

Mit 'Starten' und 'Anhalten' entscheiden Sie, ob ein Dienst eingesetzt werden soll. Mit 'Aktualisieren' sind Sie in der Lage, den aktuellen Status zu prüfen, falls dies nicht automatisch geschieht. 'Auf Standardwert zurücksetzen' dient der Wiederherstellung der Standardeinstellungen, das ist der Zustand nach der Installation. 'Dienst aktivieren' erscheint nur, wenn der Dienst derzeit deaktiviert ist. 'Alle Dienste auf Standardwert zurücksetzen' versetzt alle Dienste in den ursprünglichen Zustand, wie er nach der Installation ist. Mit 'Beenden' speichern Sie die Systemkonfiguration.

Achtung

Editieren der Runlevel-Einstellungen
Fehlerhafte Einstellungen von Systemdiensten und Runleveln können Ihr System unbrauchbar machen. Informieren Sie sich vor einer Änderung dieser Einstellungen über die möglichen Folgen, um die Funktionsfähigkeit Ihres Systems zu gewährleisten.

Achtung

SuSEconfig, /etc/sysconfig und /etc/rc.config

Die wesentliche Konfiguration von SuSE Linux nehmen Sie über die Konfigurationsdateien unter `/etc/sysconfig` vor. Die Datei `/etc/rc.config`, die bis SuSE Linux 8.0 für die Systemkonfiguration genutzt wurde, wird „leer" beibehalten, damit Ihren selbsterstellten Skripten Ihre eigenen Einstellungen nicht verlorengehen und weiterhin global ausgewertet werden können.

Auf die Dateien in `/etc/sysconfig` wird nur gezielt von einzelnen Skripten zugegriffen; dadurch wird gewährleistet, dass die Netzwerkeinstellungen auch nur von dem Netzwerk-Skripten ausgewertet werden müssen.

Darüber hinaus werden viele weitere Konfigurationsdateien des Systems in Abhängigkeit von den Dateien in `/etc/sysconfig` generiert; diese Aufgabe erledigt SuSEconfig. So wird beispielsweise nach einer Änderung der Netzwerkkonfiguration die Datei `/etc/host.conf` neu erzeugt, da sie abhängig von der Art der Konfiguration ist.

Wenn Sie Änderungen an den genannten Dateien vornehmen, müssen Sie nachfolgend immer SuSEconfig aufrufen, so dass die neuen Einstellungen

auch an allen relevanten Stellen wirksam werden. Verändern Sie die Konfiguration mit YaST2, brauchen Sie sich darum nicht explizit zu kümmern; YaST2 startet automatisch SuSEconfig, wodurch die betroffenen Dateien auf den aktuellen Stand gebracht werden.

Dieses Konzept ermöglicht es, grundlegende Änderungen an der Konfiguration des Rechners vornehmen zu können, ohne die Maschine neu booten zu müssen. Da manche Einstellungen sehr tiefgreifend sind, müssen jedoch unter Umständen einige Programme neu gestartet werden, um die Änderungen wirksam werden zu lassen.

Durch Verwendung der Kommandos

```
erde:~ #  rcnetwork stop
erde:~ #  rcnetwork start
```

wird erreicht, dass die von der Änderung betroffenen Netzwerk-Programme neu gestartet werden. Wie Sie sehen, können die Init-Skripten auch von Hand aufgerufen werden.

Generell ist für das Konfigurieren des Systems folgender Weg zu empfehlen:

- Bringen Sie das System in den „single user mode“ (Runlevel 1):

  ```
  erde:~ #  init 1
  ```

- Nehmen Sie die gewünschten Änderungen an den Konfigurationsdateien vor. Dies entweder kann mit einem Texteditor geschehen oder besser mit dem Sysconfig-Editor von YaST2; vgl. in Abschnitt *Systemkonfiguration mit dem YaST2 Sysconfig-Editor* auf der nächsten Seite.
- Führen Sie SuSEconfig aus, um die Änderungen in die verschiedenen weiteren Konfigurationsdateien eintragen zu lassen. Dies geschieht automatisch, wenn Sie YaST2 verwendet haben, um den Runlevel zu setzen.
- Bringen Sie das System in den vorherigen Runlevel zurück (hier im Beispiel 3):

  ```
  erde:~ #  init 3
  ```

Diese Vorgehensweise ist natürlich nur bei sehr weitreichenden Änderungen an den Einstellungen des Systems erforderlich (z. B. Netzwerkkonfiguration); bei einfachen Aufgaben ist es nicht erforderlich, für die Administration in den „single user mode“ zu wechseln; jedoch stellen Sie damit sicher, dass

auch wirklich alle von der Änderung betroffenen Programme neu gestartet werden.

Tipp

Sie können die automatische Konfiguration via SuSEconfig *global* abschalten, indem Sie die Variable ⟨*ENABLE_SUSECONFIG*⟩ in `/etc/sysconfig/suseconfig` auf `no` setzen. Wollen Sie den Installationssupport in Anspruch nehmen, muss ⟨*ENABLE_SUSECONFIG*⟩ allerdings auf `yes` gesetzt sein. Einzelne Teile der Autokonfiguration können auch gezielt deaktiviert werden.

Tipp

Systemkonfiguration mit dem YaST2 Sysconfig-Editor

Im Verzeichnis `/etc/sysconfig` sind die Dateien mit den wichtigsten Einstellungen für SuSE Linux hinterlegt (ehemals in der Datei `/etc/rc.config` zentral verwaltet). Der YaST2 Sysconfig-Editor stellt alle Einstellmöglichkeiten übersichtlich dar. Die Werte können geändert und anschließend in die einzelnen Konfigurationsdateien übernommen werden. Im Allgemeinen ist das manuelle Editieren allerdings nicht notwendig, da bei der Installation eines Paketes oder beim Einrichten eines Dienstes etc. die Dateien automatisch angepasst werden.

Achtung

Änderungen in den `/etc/sysconfig/*`-Dateien
Ihre Änderungen in `/etc/sysconfig/*` haben tiefgreifende Folgen für Ihr gesamtes System. Bitte informieren Sie sich vor jeder Änderung ausreichend über die möglichen Folgen. So stellen Sie sicher, dass Ihr System funktionsfähig bleibt.

Achtung

Skripte und Variablen

Im Folgenden werden die einzelnen Parameter des Systems und ihre Einstellungen *in Auswahl* kurz beschrieben. Wenn Sie die Konfigurationsdateien

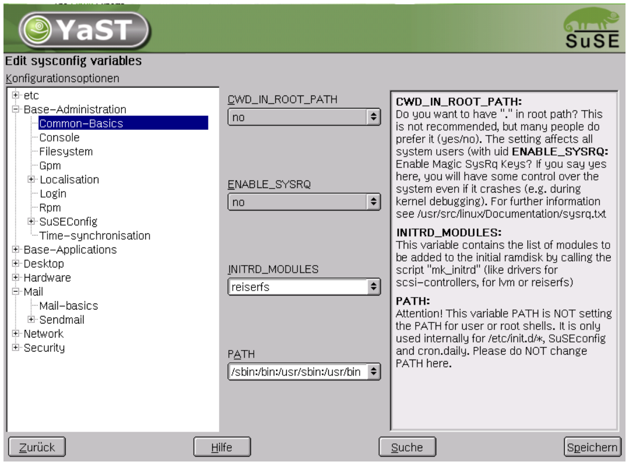


Abbildung 11.1: *YaST2: Konfiguration des sysconfig-Editors*

in `/etc/sysconfig` *nicht* mit YaST bearbeiten, achten Sie darauf, dass Sie einen leeren Parameter als zwei aufeinander folgende Anführungszeichen schreiben (z. B. ⟨*KEYTABLE=""*⟩) und Parameter, die Leerzeichen enthalten, in Anführungsstriche einschließen. Bei Variablen, die nur aus einem Wort bestehen, sind die Anführungszeichen nicht notwendig.

Hinweis

Plattformspezifische Variablen in `/etc/sysconfig`
Die hier vorgestellten Variablen und Dateien in `/etc/sysconfig` sind als der kleinste gemeinsame Nenner aller unterstützten Plattformen konzipiert. Unter Umständen finden Sie hier Variablen, die es auf Ihrer Plattform nicht gibt. Andere Variablen, die nur auf bestimmten Plattformen vorkommen, fehlen möglicherweise. Hier verweisen wir auf die Dokumentation innerhalb der `/etc/sysconfig` Dateien.

Hinweis

Einstellungen in den Dateien in /etc/sysconfig

`3ddiag` Für 3Ddiag.

`SCRIPT_3D="switch2mesasoft"`
Skript festlegen, das die notwendigen symbolischen Links für die richtigen OpenGL-Bibliotheken und -Erweiterungen anlegt. Mögliche Werte

für die in /usr/X11R6/bin befindlichen Skripte sind:

no – Kein Skript ausführen

switch2mesasoft – Emulation der Mesa-Software (funktioniert mit allen Grafikkarten)

switch2mesa3dfx – Mesa/Glide

switch2nvidia_glx – XFree86 4.x/NVIDIA_GLX (NVIDIA_GLX/NVIDIA_kernel)

switch2xf86_glx – XFree86 4.x/DRI

Mit 3Ddiag lässt sich die richtige Einstellung herausfinden .

SuSEfirewall2 Firewall-Aktivierung; vgl. die Beschreibung in Paket SuSEfirewall2.

amavis Aktivierung des AMaViS Virenscanners in Sendmail oder Postfix.

USE_AMAVIS="yes"
Hier aktivieren Sie AMaViS. SuSEconfig wird eine passende Sendmail oder Postfix Konfiguration erstellen. Mehr Details lesen Sie im README.SuSE des AMaViS Pakets.

apache Konfiguration des Apache Webservers. Diese Aufstellung umfasst lediglich solche Einstellungen, die standardmässig gesetzt oder für das Verständnis des Apache unerlässlich sind. Für alle anderen Variablen bzw. Module und deren Funktionssweisen verweisen wir auf die Apache Dokumentation, die Sie mit YaST2 als Paket apache-doc installieren können oder im WWW unter den folgenden URLs finden: http://httpd.apache.org/docs/ und http://modules.apache.org

HTTPD_PERFORMANCE="slim"
Hier legen Sie fest, wieviele Clients von Ihrem Server bedient werden können. Sie haben die Auswahl aus den Klassen „slim“, „mid“, „thick“ und „enterprise“. SuSEconfig stimmt die MinSpareServers, MaxSpareServers, StartServers und MaxClients in der Apache-Konfiguration entsprechend /sbin/conf.d/SuSEconfig.apache.

HTTPD_START_TIMEOUT="2"
Hier setzen Sie den Zeitrahmen (in Sekunden), innerhalb dessen das Startskript feststellt, ob der http Prozess fehlerfrei gestartet werden konnte. Für den Fall, dass Sie mod_ssl verwenden und Ihr SSL-Zertifikat passwortgeschützt ist, erhöhen Sie diesen Wert.

HTTPD_SEC_ACCESS_SERVERINFO="no"
Diese Einstellung aktiviert die Module mod_status und mod_info, die jeweils über den Status, die Performance und die Konfiguration Ihres Servers Auskunft geben.

HTTPD_SEC_SAY_FULLNAME="no"
Welche Informationen sollen über den Server nach aussen in Form einer Fußzeile bei servergenerierten Dokumenten (z. B. Fehlermeldungen) weitergegeben werden? Sie haben die Wahl zwischen `yes` für Versionsnummer und Servernamen, `no` für keine Information und `email` für Versionsnummer, Name und `mailto:`-Anweisung an den Administrator des Servers. Diese Variable korreliert mit der `ServerSignature` Direktive des Apache.

HTTPD_SEC_SERVERADMIN=""
Bitte tragen Sie an dieser Stelle die E-Mailadresse des Serveradministrators ein. Haben Sie ⟨*HTTPD_SEC_SAY_FULLNAME*⟩ auf `yes` gesetzt, wird diese Angabe nach aussen weitergeleitet. Bleibt dieser Eintrag leer, wird als Mailadresse standardmässig `webmaster@$HOSTNAME` verwendet. ⟨*HOSTNAME*⟩ (der vollständige Hostname des Servers) wird in der Datei `/etc/HOSTNAME` festgelegt. ⟨*HTTPD_SEC_SERVERADMIN*⟩ entspricht der `ServerAdmin` Direktive des Apachen. `ServerAdmin` Direktiven in den `VirtualHost` Statements werden durch Ihren Eintrag an dieser Stelle nicht verändert – ebensowenig wie der Eintrag des SSL Virtual Hosts.

HTTPD_SEC_PUBLIC_HTML="yes"
Sollen `public_html` Verzeichnisse im Homeverzeichnis der Benutzer zugänglich gemacht werden? Beantworten Sie diese Frage mit `yes`, so können Sie die weiteren Einstellungen in `/etc/httpd/suse_public_html.conf` vornehmen.

HTTPD_CONF_INCLUDE_FILES=""
Durch Leerzeichen voneinander getrennt, geben Sie hier Dateien an, die von `/etc/httpd/httpd.conf` übernommen werden sollen. Auf diese Weise können Sie z. B. `VirtualHost` Statements neu anlegen, ohne extra `/etc/httpd/httpd.conf` ändern zu müssen. Solange SuSEconfig über den MD5-Summen Mechanismus keine Änderung von `/etc/httpd/httpd.conf` feststellt, wird diese Datei bei der Apache Konfiguration nicht angerührt werden müssen.

HTTPD_AWSTATS_COMBINED_LOG="yes"
Soll Apache ein extra Logfile anlegen, das von awstats (engl. *Advanced Web Statistics*) ausgewertet wird?

HTTPD_DDT="yes"
Das DDT Admin CGI wird aktiviert. Sie können es verwenden, um auf einem lokalen DDT (engl. *Dynamic DNS Tools*) Server Accounts anzulegen und zu verwalten.

MAILMAN_APACHE="yes"
Soll das Mailman Webfrontend zur Verwaltung von Mailinglisten akti-

viert werden?

HTTPD_SEC_MOD_MIDGARD="yes"
Aktivieren des `midgard` Moduls. Midgard ist ein Open Source Content Management System.

HTTPD_SEC_MOD_PERL="yes"
Aktivieren des `mod_perl` Moduls

HTTPD_SEC_MOD_PHP="yes"
Aktivieren des `mod_php` Moduls

HTTPD_SEC_MOD_PYTHON="yes"
Wollen Sie das Python-Modul des Apache aktivieren? `yes` ist hier die Voreinstellung.

HTTPD_SEC_NAGIOS="yes"
Erlauben Sie den Zugang zum Nagios Webinterface. Sie konfigurieren es unter `/etc/httpd/nagios.conf`.

HTTPD_SEC_MOD_SSL="no"
Hier aktivieren Sie das SSL Modul. Die Voreinstellung ist `no`, da Sie einige Vorarbeiten leisten müssen, bevor SSL fehlerfrei verwendbar ist.
Erstellen Sie ein Serverzertifikat. Ein Testzertifikat legen Sie an, indem Sie folgende Befehle in dieser Reihenfolge als `root` ausführen:

```
cd /usr/share/doc/packages/mod_ssl
./certificate.sh
```

Setzen Sie ⟨*ServerName*⟩ im `VirtualHost _default_:443` der `httpd.conf` auf den vollständigen Servernamen (engl. *Fully Qualified Domain Name*) (siehe ⟨*HOSTNAME*⟩ `/etc/HOSTNAME`).
Erhöhen Sie ⟨*HTTPD_START_TIMEOUT*⟩, wenn Ihr Serverzertifikat passwortgeschützt ist (siehe oben).

ZOPE_PCGI="no"
Sollen Anfragen von Zope über das PCGI-Interface von Apache abgewickelt werden? Belassen Sie diese Variable auf der Voreinstellung `no`, startet Zope als Standalone Webserver. Setzen Sie hier `yes`, müssen Sie Apache installiert haben, um PCGI verwenden zu können. Mehr Optionen liegen in `/etc/sysconfig/zope`.

ZOPE_KEEP_HOMES="yes"
Sollten Zope-Anfragen über apache-pcgi abgewickelt werden und ⟨*ZOPE_KEEP_HOMES*⟩ auf `yes` gesetzt sein, werden die Homeverzeichnisse der Benutzer von Apache gehandhabt.

argoups Die Konfiguration für argoups. Dieses Paket bietet die Möglichkeit, das System über einen speziellen Daemon kontrolliert herunterfah-

ren zu können, falls die USV (Unterbrechnungsfreie Stromversorgung) einen Stromausfall meldet.

ARGO_TYPE="local"
Geben Sie hier den Verbindungstyp zum zu überwachenden System ein. Wenn Sie ein System „fernüberwachen" möchten, tragen Sie dessen Namen bei ⟨*ARGO_REMOTESERVER*⟩ ein.

ARGO_REMOTESERVER=""

ARGO_TTY="/dev/ttyS0"
Über welchen seriellen Port besteht die Verbindung zu ArgoUPS?

ARGO_USERTIME="2"
Wie lang (in Minuten) nach dem Stromausfall soll das Skript aus ⟨*ARGO_USERFILE*⟩ ausgeführt werden?

ARGO_USERFILE="/usr/sbin/argoblackout"

ARGO_SHUTDOWN="8"
Wann soll danach der Shutdown eingeleitet werden?

argus Server für Argus (Netzwerkmonitor).

ARGUS_INTERFACE="eth0"
Das von Argus zu überwachende Interface.

ARGUS_LOGFILE="/var/log/argus.log"
Die Argus-Logdatei. Diese Datei kann sehr groß werden!

autofs Mit diesem Daemon ist es möglich, sowohl über NFS erreichbare Verzeichnisse als auch lokale Verzeichnisse (CD-ROM-Laufwerke, Disketten etc.) automatisch zu mounten.

AUTOFS_OPTIONS=""
Optionen für autofs, z. B. "`--timeout 60`". Die `-timeout` Option legt fest, nach welchem Zeitraum (in Sekunden) Verzeichnisse automatisch wieder ausgehängt werden sollen (engl. *unmount*).

autoinstall AutoYaST2 der Auto-Installer von YaST2.

REPOSITORY="/var/lib/autoinstall/repository"
Ablage für alle „Profiles". Dies sind die Kontrolldateien, die die Konfigurationsbeschreibungen für die zu installierenden Hosts beinhalten.

CLASS_DIR="/var/lib/autoinstall/classes"
Sie können bei der Erstellung von Profilen/Kontrolldateien für komplexe Installationsszenarien mit vielen Hosts zur Vereinfachung Klassen definieren, die verschiedene Hosttypen und -gruppen abbilden. YaST2 legt diese unter `/var/lib/autoinstall/classes` ab.

PACKAGE_REPOSITORY=""
Dieses Verzeichnis enthält die Installationsdaten/Pakete für SuSE Linux.

backup Kopien der RPM-Datenbank.

RPMDB_BACKUP_DIR="/var/adm/backup/rpmdb"
Legt fest, wohin cron.daily Backups der RPM-Datenbank schreiben soll; wenn keine Backups gewünscht werden, diese Variable auf `""` setzen.

MAX_RPMDB_BACKUPS="5"
Legt die Anzahl der Backups der RPM-Datenbank fest.

RCCONFIG_BACKUP_DIR="/var/adm/backup/rpmdb"
In das hier angegebene Verzeichnis legt cron.daily die Backups von Ihrer `/etc/rc.config` und den Dateien unter `etc/sysconfig/` ab. Wann immer diese Dateien geändert werden, wird der nächste cron.daily-Lauf Backups erzeugen. Wünschen Sie keine Backups, setzen Sie diese Variable auf `""` .

MAX_RCCONFIG_BACKUPS="5"
Hier legen Sie fest, wieviele Backups von den Dateien unter `/etc/sysconfig` und von `/etc/rc.config` vorgehalten werden.

clock Zeiteinstellungen.

GMT=""
Wenn Ihre Hardware-Uhr auf GMT (*Greenwich Mean Time*) eingestellt ist, setzen Sie diese Variable auf `-u`, anderenfalls setzen Sie die Variable auf `--localtime`. Diese Einstellung ist relevant für das automatische Umstellen von Sommer- auf Winterzeit und umgekehrt.

TIMEZONE=""
Die Zeitzone, in der Sie wohnen bzw. den Rechner betreiben. Diese Einstellung ist auch wichtig für die automatische Umstellung von Sommer- auf Winterzeit und umgekehrt. Damit wird `/usr/lib/zoneinfo/localtime` gesetzt.

console Einstellungen für die Konsole.

FB_MODULES=""
Wollen Sie Framebuffer-Treibermodule zu Ihrem Kernel hinzuladen? Vor einer Entscheidung für das Laden der Module sollten Sie bedenken, dass Ihre Einstellungen nicht funktionieren, wenn vesafb bereits aktiv ist. Weiterhin ist es vorteilhaft, Framebufferunterstützung direkt in den Kernel hineinkompiliert zu haben. Schließlich haben manche XFree86-Treiber (inbesondere der XFree86-4.x Serie) im Framebuffer Textmodus Probleme.

FBSET_PARAMS=""
Bietet Ihr Kernel Framebufferunterstützung (oder wird diese als Modul geladen), werden Sie die Auflösung oder andere Parameter ändern wollen. Geben Sie fbset die entsprechenden Parameter mit (Details: `man fbset` und/oder `fbset -h`).

Achtung

Einstellen der Framebuffer Parameter
Die möglichen Einstellungen sind stark von Ihrer speziellen Hard- und Software abhängig. Falsche Entscheidungen können unter Umständen Ihren Monitor beschädigen. Bitte beachten Sie daher Folgendes:

vesafb bietet (noch) keine Unterstützung für den Wechsel des Displaymodus.

Wählen Sie keine Displaymodi, die von Ihrem Monitor nicht unterstützt werden.

Achtung

CONSOLE_FONT=""
Der Font, der für die Konsole beim Booten geladen wird. Nicht alle Fonts unterstützen z. B. die deutschen Umlaute oder andere 8-Bit-Zeichen! Zusatzeinstellungen sind: ⟨*CONSOLE_SCREENMAP*⟩, ⟨*CONSOLE_UNICODEMAP*⟩ und ⟨*CONSOLE_MAGIC*⟩.

CONSOLE_UNICODEMAP=""
Manche Fonts haben keine eigene Unicode Map. Geben Sie hier explizit das von Ihnen gewünschte Unicode Mapping an. Sie finden diese Dateien unter `/usr/share/kbd/unimaps/`. Im Normalfall wird diese Option allerdings nich benötigt.

CONSOLE_SCREENMAP=""
Muss der von Ihnen verwendete Font in Unicode-Zeichensatz umgesetzt werden? Geben Sie hier die passende Screenmap an. Screenmaps finden Sie unter `/usr/share/kbd/consoletrans/`.

CONSOLE_MAGIC=""
Die Konsole muss je nach verwendetem Font unter Umständen mit ⟨*CONSEOLE_MAGIC*⟩ initialisiert werden. Im Normalfall müssen Sie hier keine Änderungen vornehmen.

SVGATEXTMODE="80x25"
Das zugehörige Paket `svgatext` erlaubt die Einstellung höherer Textauflösungen (bis zu 160x60) mit SVGA-Karten. Diese Variable enthält einen gültigen Wert aus `/etc/TextConfig`. Bitte passen Sie diese Datei den Gegebenheiten Ihrer Grafikkarte entsprechend an. Wie dies

zu erreichen ist, erfahren Sie unter /usr/share/doc/packages/svgatext. Standardeinstellung für ⟨*SVGATEXTMODE*⟩ ist „80x25“. SVGATextMode Auflösungen werden in den Runlevels 1,2,3 und 5 verwendet.

cron Tägliche Wartungsarbeiten am System.

Der Cron-Daemon startet zu vorgegebenen Zeiten automatisch gewisse Programme. Seine Aktivierung ist auf Rechnern, die rund um die Uhr laufen, dringend zu empfehlen. Eine Alternative bzw. Ergänzung ist der AT-Daemon.

Hinweis

Es gibt eine Reihe von Systemeinstellungen, die es erfordern, dass regelmäßig bestimmte Programme gestartet werden. Daher sollte auf jedem System der Cron-Daemon aktiviert werden.

Hinweis

MAX_DAYS_IN_TMP="0"
Es wird täglich geprüft, ob es in den tmp-Verzeichnissen (vgl. ⟨*TMP_DIRS_TO_CLEAR*⟩) Dateien gibt, auf die länger als angegeben nicht zugegriffen wurde (in Tagen). Wurde auf eine Datei in einem dieser Verzeichnisse länger als angegeben nicht mehr zugegriffen, wird sie gelöscht.

Dieser Mechanismus kann mit "" oder 0 (Vorgabe) abgeschaltet werden. Diese Variable sollte gesetzt werden, wenn mehrere Benutzer das System verwenden, um ein Überlaufen der tmp-Verzeichnisse zu verhindern.

TMP_DIRS_TO_CLEAR="/tmp /var/tmp"
Angabe derjenigen Verzeichnisse, die täglich nach „alten“ Dateien durchsucht werden sollen; vgl. ⟨*MAX_DAYS_IN_TMP*⟩.

OWNER_TO_KEEP_IN_TMP="root"
Die Dateien der hier angegebenen Systembenutzer sollen auch dann nicht aus den tmp-Verzeichnissen gelöscht werden (vgl. ⟨*TMP_DIRS_TO_CLEAR*⟩), wenn auf sie länger als angegeben nicht mehr zugegriffen wurde.
Achtung: Wenn ⟨*CLEAR_TMP_DIRS_AT_BOOTUP*⟩ auf yes steht, wird dieser Eintrag hier *nicht* beachtet!

CLEAR_TMP_DIRS_AT_BOOTUP="no"
Setzen Sie diese Variable auf yes, wenn alle Dateien und Unterverzeichnisse in den temporären Verzeichnissen, die in

⟨*TMP_DIRS_TO_CLEAR*⟩ genannt sind, gelöscht werden sollen (`rm -fr`).
Achtung: Wenn diese Variable auf `yes` gesetzt wird, werden die Einträge in ⟨*OWNER_TO_KEEP_IN_TMP*⟩ *nicht* beachtet; alle Dateien werden ausnahmslos gelöscht!

`DELETE_OLD_CORE="no"`
Corefiles sind Abbilder der Speicherbelegung von Programmen, die wegen einer Speicherschutzverletzung abgebrochen wurden; diese Abbilder dienen der Fehlersuche. Hier können Sie einstellen, dass regelmäßig nach etwaigen alten Corefiles gesucht wird und diese automatisch gelöscht werden. Gleichzeitig muss das Paket `findutils-locate` installiert und ⟨*RUN_UPDATEDB*⟩ auf `yes` gesetzt sein.

`MAX_DAYS_FOR_CORE="7"`
Legt fest, wie alt Corefiles maximal werden dürfen (in Tagen), bevor sie automatisch gelöscht werden.

`REINIT_MANDB="yes"`
Wenn die Manpage-Datenbanken (mandb und whatis) von cron.daily täglich neu angelegt werden sollen.

`DELETE_OLD_CATMAN="yes"`
Sollen veraltete vorformatierte Manual-Pages in `/var/catman` gelöscht werden?

`CATMAN_ATIME="7"`
Wie lang (in Tagen) sollen vorformatierte Manual-Pages aufgehoben werden, bevor sie gelöscht werden?

`dhcpd` Konfiguration des DHCP-Servers

`DHCPD_INTERFACE="eth0"`
Interface/s, auf dem/denen der DHCP-Server lauschen soll.

`DHCPD_RUN_CHROOTED="yes"`
Soll dhcpd in einem „chroot jail" betrieben werden? Lesen Sie hierzu bitte das README.SuSE zu dhcp unter `/usr/share/doc/packages/dhcp/README.SuSE`.

`DHCPD_CONF_INCLUDE_FILES=""`
Die Datei `dhcpd.conf` kann `include`-Statements enthalten. Geben Sie unter ⟨*DHCPD_CONF_INCLUDE_FILES*⟩ alle Dateien an, die Sie inkludieren wollen. Auf diese Weise werden *alle* Ihre `.conf` Dateien ebenso wie `/etc/dhcpd.conf` in das Chroot-Verzeichnis (`\$chroot/etc/`) kopiert.

DHCPD_RUN_AS="nobody"
Legen Sie fest, als welcher Benutzer dhcpd gestartet wird. Bleibt diese Variable leer oder geben Sie `root` an, wird dhcpd als `root` gestartet. Mit `nobody` startet er als `nobody` der Gruppe `nogroup`.

DHCPD_OTHER_ARGS=""
Hier geben Sie dhcpd weitere Argumente mit (siehe `man dhcpd`).

dhcrelay Konfiguration des DHCP-Relay-Agents. Er dient als „Vermittler“ zwischen Subnetzen mit und ohne eigenem DHCP-Server. DHCP- (und Bootp-) Anfragen aus einem Subnetz ohne eigenen Server leitet er an einen oder mehrere DHCP-Server im Netz weiter und übermittelt deren Antworten.

DHCRELAY_INTERFACES=""
Interfaces, auf denen der DHCP-Relay-Agent lauschen soll. Bitte trennen Sie die Einträge durch Leerzeichen.

DHCRELAY_SERVERS=""
An welche DHCP-Server kann sich der DHCP-Relay-Agent wenden? Tragen Sie hier einen oder mehrere Server durch Leerzeichen getrennt ein.

displaymanager Displaymanager konfigurieren.

DISPLAYMANAGER=""
Diese Variable legt fest, welcher Displaymanager zum Anmelden („Login“) verwendet werden soll. Mögliche Werte sind `console`, `xdm` (traditioneller Displaymanager des X Window System), `kdm` (Displaymanager von KDE), `gdm` (Displaymanager von GNOME) oder `wdm` (der „WINGs Display Manager“).

DISPLAYMANAGER_REMOTE_ACCESS="no"
Wollen Sie einen Remotezugriff auf Ihren Displaymanager erlauben? Die Standardeinstellung ist `no`.

DISPLAYMANAGER_STARTS_XSERVER="yes"
Soll der Displaymanager einen lokalen X-Server starten? Erlauben Sie ausschliesslich Remotezugriff, ist diese Variable auf `no` zu setzen.

KDM_SHUTDOWN="auto"
Hier legen Sie fest, von wem das System in kdm heruntergefahren werden darf. Mögliche Werte sind `root`, `all`, `none`, `local` und `auto`.

KDM_USERS=""
Tragen Sie, durch Leerzeichen getrennt, die Liste der Benutzer ein, für die in kdm Icons angezeigt werden sollen. Nehmen Sie hier keine eigenen Einträge vor, werden die Standardeinstellungen des Systems verwendet.

KDM_BACKGROUND=""
Hier lässt sich ein Hintergrund für kdm angeben.

KDM_GREETSTRING=""
Wünschen Sie eine besondere Begrüßung durch kdm?

dracd Einstellungen für den dracd Daemon und das Mail-Relaying durch „POP-before SMTP."

DRACD_RELAYTIME="5"
Postfix hält auf dem POP-Server für eine bestimmte Zeitspanne die IP-Adresse eines authentifizierten Hosts vor und erlaubt das Versenden von Mails von eben diesem Host. Nach dieser Zeit wird der Eintrag gelöscht und eine neue Authentifizierung erforderlich. Die Angabe erfolgt in Minuten.

DRACD_DRACDB="/etc/postfix/dracd.db"
Hier ist die `dracdb` zu finden.

dvb DVB-Karte

DVB_SOUND_CHIP="ti"
Soundchip auf der DVB-Karte festlegen; `ti` oder `crystal`.

hardware Hardware-Einstellungen.

DEVICES_FORCE_IDE_DMA_ON=""
DMA bei den genannten Geräten einschalten.

DEVICES_FORCE_IDE_DMA_OFF=""
DMA bei den genannten Geräten abschalten.

hotplug Einstellungen zu Hotplug.

HOTPLUG_DEBUG="default"
Mit dieser Variable kontrollieren Sie die Menge an (Fehler-)Meldungen, die der hotplug Service an syslog meldet. `default`, `""` , oder `no` bewirken eine moderate Menge an Meldungen, `off` lässt hotplug „verstummen" und `verbose` oder `yes` geben einige zusätzliche Debugmeldungen weiter. `max` führt dazu, dass `syslog` mit Meldungen „überschwemmt" wird.

HOTPLUG_START_USB="yes"
Hier starten oder stoppen Sie USB Hotplug.

Hinweis

USB Hotplug deaktivieren
Sollten Sie USB Hotplug deaktivieren und die USB-Eingabegeräte als Modul geladen haben, wird Ihre Tastatur nicht mehr reagieren, da Sie die Tastaturunterstützung auf diese Weise mit deaktivieren.

Hinweis

`HOTPLUG_USB_HOSTCONTROLLER_LIST="usb-uhci uhci usb-ohci ehci-hcd"`
Hier legen Sie die „Probing"-Reihenfolge der Hostcontroller-Treiber fest.

`HOTPLUG_USB_MODULES_TO_UNLOAD="scanner"`
Diese Module werden bei einem USB „remove" entfernt. Für manche Hardware ist eine Reinitialisierung durchaus sinnvoll.

`HOTPLUG_USB_NET_MODULES="pegasus usbnet catc kaweth CDCEther"`
Wird eines dieser Module in/aus dem Speicher geladen, nimmt das System an, dass es sich hierbei um ein Netzwerkgerät handelt und erstellt eine Hardwarebeschreibung für das folgende „net event".

`HOTPLUG_START_NET="yes"`
Aktivieren/Deaktivieren Sie NET Hotplug Event Handling.

`HOTPLUG_NET_DEFAULT_HARDWARE=""`
Bis hotplug selbständig erkennt, welcher Typ Hardware sich hinter einem Netzwerkinterface verbirgt, werden bei USB oder PCI Hotplug Events Hardwarebeschreibungen erstellt, die zum NET Event ausgelesen werden. Gleichzeitiges Hinzufügen mehrerer Hotplug Geräte kann Race Conditions auslösen. Sollte die automatische Erkennung neuer Geräte nicht funktionieren, wird beim Aufruf von if{up,down} der Inhalt von ⟨*HOTPLUG_NET_DEFAULT_HARDWARE*⟩ ausgewertet. Tragen Sie hier ein, was Sie als NIC (engl. *Network Interface Card*) verwenden: `pcmcia`, `usb` oder `firewire`.

`HOTPLUG_NET_TIMEOUT="8"`
Geben Sie hier einen Wert an, wie lange (in Sekunden) auf eine Hardwarebeschreibung von einem USB oder PCI Hotplug Event gewartet werden soll. Nimmt diese Variable den Wert `0` an, wird automatisch ⟨*HOTPLUG_NET_DEFAULT_HARDWARE*⟩ ausgewertet. Die Voreinstellung von acht Sekunden berücksichtigt den Zeitbedarf mancher PCMCIA Netzwerkkarten.

`HOTPLUG_START_PCI="yes"`
Aktivieren/Deaktivieren des PCI Hotplug Event Handlings.

HOTPLUG_PCI_MODULES_NOT_TO_UNLOAD=""
Die folgenden Module sollen beim „PCI remove Event“ nicht aus dem Speicher geladen werden.

intermezzo Einstellungen zum Intermezzo-Filesystem.

EXCLUDE_GID="63"
Geben Sie hier an, welche Gruppe von der Replikation ausgenommen werden soll.

irda IrDA ist die Infrarot-Schnittstelle, die bei Notebooks häufig anzustellen ist.

IRDA_PORT="/dev/ttyS1"
Momentan wird nur der serielle Modus (UART [SIR]) in der Standard-Konfiguration unterstützt. Im BIOS-Setup ist der verwendete serielle Port nachzusehen. Sollten Sie einen unterstützten FIR Chipsatz haben, legen Sie das entsprechende Kernelmodul (z. B. `toshoboe`) fest. FIR muss zuerst in den BIOS-Einstellungen aktiviert werden. In einzelnen Fällen, kann es nötig sein, den seriellen Port via `setserial /dev/ttyS<x> uart none` zu deaktivieren.

isdn/ Alle wichtigen Skripte zu ISDN.

ispell Überprüfung der Rechtschreibung.

ENGLISH_DICTIONARY="system american british"
SuSEconfig.ispell verwaltet einen symbolischen Link vom „englischen“ Wörterbuch auf eines der beiden von `american` oder `british`. Ist sowohl ispell-american als auch ispell-british installiert, greift ⟨*ENGLISH_DICTIONARY*⟩. Der Wert `system` verweist auf die Standardsprache des Systems (festgelegt in `/etc/sysconfig/language` unter ⟨*RC_LANG*⟩), so diese eine der beiden englischen Sprachen ist. Andernfalls hat `system` keinen Effekt. Ein symbolischer Link wird auf das erste installierte Wörterbuch dieser Liste gesetzt.

java Einstellungen zur Java-Konfiguration

CREATE_JAVALINK="yes"
SuSEconfig kann für Sie die `/usr/lib/java` und `/usr/lib/jre` Links zum passenden JDK (engl. *Java Development Kit*) und JRE (engl. *Java Runtime Environment*) anlegen, wenn Sie den Wert dieser Variable auf `yes` setzen. Ziehen Sie die manuelle Konfiguration vor, setzen Sie ⟨*CREATE_JAVALINK*⟩ auf `no`.

JAVA_JRE_THREADS_TYPE="green"
Konfiguration des `java-jre` Pakets. Wenn Sie *echtes* Multithreading wünschen, setzen Sie diese Variable auf `native`. Dies macht z. B. in Kombination mit SMP Systemen Sinn.

joystick Einstellungen zur Joystick-Konfiguration.

GAMEPORT_MODULE_0=""
Name des Gameport-Moduls, z. B. `ns558` für einen betagten Gameport.

JOYSTICK_MODULE_0=""
Normalerweise `analog`.

JOYSTICK_MODULE_OPTION_0=""
Zum Beispiel "`js=gameport`" für `ananlog`.

JOYSTICK_CONTROL_0=""
Zum Beispiel `yes`.

JOYSTICK_CONTROL_PORT_0=""
Soundkarten wie ens1371 benötigen hier eine Port-Adresse; üblicherweise `0x200`.

kernel Kernel.

INITRD_MODULES=""
Die Namen der Module, die per `mk_initrd` zur Initial Ramdisk hinzugefügt werden müssen. (z. B. Treiber für SCSI-Controller, LVM oder ReiserFS) ; vgl. Abschnitt *Booten mit der initial ramdisk* auf Seite 202 .

SHMFS=""
Hier übergeben Sie den Größenparameter für das Mounten des shmfs Filesystems. Standardmäßig verwendet der Kernel hier 50% des verfügbaren Speichers. Dies kann, abhängig vom individuellen Setup, manchmal nicht ausreichend sein.

keyboard Einstellungen für die Tastatur.

KEYTABLE="de-latin1-nodeadkeys"
Definiert die Tastaturbelegung. Bei Verwendung einer US-Tastatur kann diese Variable leer bleiben.

KBD_RATE="24.0"
Bestimmt die Geschwindigkeit der automatischen Tastaturwiederholung. Mögliche Eingaben sind von zweimal bis zu 30 mal pro Sekunde. Damit diese Einstellung wirkt, muss gleichfalls die Dauer der Verzögerung (vgl. ⟨*KBD_DELAY*⟩) festgelegt werden!

KBD_DELAY="500"
Mögliche Werte: `250`, `500`, `750` und `1000`. Hier können Sie die Verzögerung einstellen, nach der die automatische Wiederholfunktion einsetzt. Der Wert ist in Millisekunden, das Raster ist jedoch nicht sehr genau. Sie müssen auch ⟨*KBD_RATE*⟩ einstellen!

KBD_NUMLOCK="bios"
Bei `no` wird (NumLock) beim Booten nicht eingeschaltet. Weitere mögliche Einstellungen sind `yes`, `""` oder `bios` für BIOS-Einstellung.

KBD_SCRLOCK="no"
(SrollLock) einschalten?

KBD_CAPSLOCK="no"
(CapsLock) beim Booten nicht einschalten.

KBD_DISABLE_CAPS_LOCK="no"
Soll (CapsLock) abgeschaltet werden und sich wie eine normale (Shift) Taste verhalten?

KBD_TTY="tty1 tty2 tty3 tty4 tty5 tty6"
(NumLock), (CapsLock) und (ScrollLock) kann auf bestimmte TTYs beschränkt werden; "" steht für alle TTYs.

COMPOSETABLE="clear winkeys shiftctrl latin1.add"
Hier legen Sie die zu ladende „Compose Table“ fest. Mittels „Composetable“ ist es Ihnen möglich, Sonderzeichen (Akzente, Währungssymbole etc.), die nicht direkt auf die Tastatur gelegt sind, dennoch über spezielle Tastenkombinationen einzugeben. Eine detaillierte Erklärung finden Sie unter `/usr/share/doc/packages/kbd/README.SuSE`.

language Einstellungen zu Sprache und Standort (Lokale).

RC_LANG="de_DE@euro"
Setzt `LANG` für locale; hiermit kann für die lokalen Benutzer eine Vorgabe eingestellt werden. Dieser Wert kommt solange zum Tragen, wie keine speziellen ⟨*RC_LC_**⟩-Variablen benutzt werden.
Die einschlägigen `sysconfig`-Variablen lauten: ⟨*RC_LC_ALL*⟩ (hiermit kann man die `LC_*` wie auch `LANG` überschreiben!), ⟨*RC_LC_MESSAGES*⟩, ⟨*RC_LC_CTYPE*⟩, ⟨*RC_LC_MONETARY*⟩, ⟨*RC_LC_NUMERIC*⟩, ⟨*RC_LC_TIME*⟩ und ⟨*RC_LC_COLLATE*⟩.
Vgl. Abschnitt *Lokale Anpassungen – I18N/L10N* auf Seite 220.

ROOT_USES_LANG="ctype"
Sollen auch für `root` die locale-Einstellungen verwendet werden? `ctype` bedeutet, dass hier der Wert von ⟨*LC_CTYPE*⟩ verwendet wird.

locate Die locate-Datenbank dient dem schnellen Auffinden von Dateien im System. – Diese Aktualisierung wird möglicherweise kurz nach

dem Booten durchgeführt, wenn Sie den Rechner *nicht* ununterbrochen laufen haben; vgl. Abschnitt *Paket cron* auf Seite 198.

RUN_UPDATEDB="no"
Einmal täglich soll die Datenbank für locate (`locate`) aktualisiert werden. Eine Detailkonfiguration des Programms updatedb kann über die folgenden Variablen erreicht werden (vgl. die Kommentare dort).

RUN_UPDATEDB_AS="nobody"
Der Benutzer, unter dessen Identität updatedb ausgeführt werden soll. Die Standardeinstellung ist hier aus Sicherheitsgründen `nobody`.

UPDATEDB_NETPATHS=""
updatedb durchsucht von sich aus nur lokale Verzeichnisse. Sie können aber selbst zu durchsuchende Netzwerkverzeichnisse festlegen.

UPDATEDB_PRUNEPATHS="/mnt /media/cdrom /tmp /usr/tmp /var/tmp /var/spool /proc /media"
Alle Verzeichnisse, die hier eingetragen werden, ignoriert updatedb bei seiner Suche.

UPDATEDB_NETUSER=""
Siehe oben; hier legen Sie den Benutzer fest, unter dessen Identität Netzpfade durchsucht werden sollen. `nobody` ist ein Beispiel.

UPDATEDB_PRUNEFS=""
updatedb kann nicht nur bestimmte Verzeichnisse ignorieren; auch Dateisystemtypen können von der Suche ausgenommen werden.

lvm Der Logical Volume Manager.

mail Einstellungen bezüglich E-Mail.

FROM_HEADER=""
`From:`-Zeile systemweit vorgeben. Wenn "", wird der FQDN verwendet; vgl. *Domain Name System* auf Seite 277.

MAIL_CREATE_CONFIG="yes"
SuSEconfig wird eine `/etc/sendmail.cf` aus den Angaben zusammenstellen, die Sie unter `sendmail` machen. Bevorzugen Sie die manuelle Konfiguration, setzen Sie diese Variable auf `no`.

NULLCLIENT=""
Ein „Nullclient" ist eine Maschine, die ausschließlich Mail versenden kann. Sie erhält keinerlei Mail aus dem Netz und kann auch lokal keine Mail zustellen. Typischerweise verwendet ein „Nullclient" POP oder NFS für den Mailbox-Zugriff.

SMTPD_LISTEN_REMOTE="no"
`yes` wird gesetzt, sobald Mails von extern angenommen werden sollen. Für einen Mailserver ist diese Einstellung ein „Muss".

mouse Maus-Einstellungen.

MOUSE=""
Die Schnittstelle, an der die Maus angeschlossen ist (z. B. /dev/ttyS0). Von YaST2 bzw. SuSEconfig wird ein Link von /dev/mouse auf das angegebene Device angelegt.

GPM_PROTOCOL=""
Das GPM-Protokoll für das unter ⟨*MOUSE*⟩ eingetragene Device. Diesen Wert legt YaST2 fest.

GPM_PARAM=" -t $GPM_PROTOCOL -m $MOUSE"
Die Startparameter für den gpm.

network Verzeichnis für Netwerkkonfigurationen.

network/config Generelle Einstellungen zur Netzwerkkonfiguration.

DEFAULT_BROADCAST="+"
⟨*DEFAULT_BROADCAST*⟩ wird ausgewertet, wenn keine andere BROADCAST Angabe gesetzt wurde. Sie können zwischen "" für keine Broadcastadresse, - für die ⟨*IPADDR*⟩ ohne Host Bits und + für die volle Angabe der ⟨*IPADDR*⟩ mit allen Host Bits wählen.

CHECK_FOR_MASTER="yes"
Dieser Eintrag bewirkt, dass ein „Master"-Interface bereits aktiviert sein muss, bevor Alias-Adressen („labelled address") aufgesetzt werden können. Technisch hat dieser Eintrag keinerlei Konsequenz, aber Benutzer von ifconfig profitieren davon.

CHECK_DUPLICATE_IP="yes"
yes bewirkt, dass das ifup-Skript prüft, ob eine IP-Adresse bereits benutzt wird. Bitte stellen Sie sicher, dass der Kernel Packet-Sockets unterstützt (⟨*CONFIG_PACKET*⟩), um die ARP Funktionalität, von der dieses Feature abhängt, zu gewährleisten. Diese Prüfung dauert eine Sekunde pro Interface, was sich bei einer großen Anzahl IP-Adressen bemerkbar machen kann.

DEBUG="no"
Generelles An-/Ausschalten von Debug-Meldungen für alle Netzwerkskripte. Selbst bei no können Sie mit der Option -o debug die Debug-Meldungen einzelner Skripte wieder aktivieren.

USE_SYSLOG="yes"
Sollen Fehlermeldungen der Konfigurationsskripte nach syslog ausgegeben werden?

MODIFY_RESOLV_CONF_DYNAMICALLY="yes"
Manche Dienste wie `ppp`, `ippp`, `dhcp-client`, `pcmcia` und `hotplug` wollen zu bestimmten Zeiten `/etc/resolv.conf` verändern. Der Standardwert ist `yes`.

MODIFY_NAMED_CONF_DYNAMICALLY="no"
Siehe ⟨*MODIFY_RESOLV_CONF_DYNAMICALLY*⟩. Sollten Sie sich hier unsicher sein, belassen Sie es bei der Standardeinstellung `no`.

network/dhcp Einstellungen zu DHCP (engl. *Dynamic Host Configuration Protocol*).

Hinweis

Um die Konfiguration eines oder mehrerer Interfaces über DHCP zu ermöglichen, muss ⟨*BOOTPROTO*⟩ in `/etc/sysconfig/network/ifcfg-<interface>` den Wert `dhcp` annehmen. Eventuell muss ⟨*STARTMODE*⟩ den Wert `onboot` zugewiesen bekommen.

Hinweis

Die meisten dieser Optionen werden nur von dhcpcd verwendet, der ISC dhclient verwendet eine eigene Konfigurationsdatei. Manche Optionen werden auch durch die Einstellungen in den `ifcfg-*`-Dateien überschrieben.

DHCLIENT_BIN=""
Welcher DHCP-Client soll verwendet werden? `dhcpcd` für den DCHP Client Daemon oder `dhclient` für den ISC dhclient? Ein leerer Eintrag bewirkt, dass zuerst versucht wird, dhcpcd zu starten. Bleibt dies ohne Erfolg, wird dhclient versucht.

DHCLIENT_DEBUG="no"
Soll DHCP Client im Debug-Modus gestartet werden? Für DHCP Client Daemon liegen die Logdateien unter `/var/log/messagesfordhcpcd`, für ISC dhclient unter `/var/log/dhclient-script`.

DHCLIENT_SET_HOSTNAME="no"
Soll der DHCP Client den Hostnamen setzen? Achten Sie bei der Einstellung `yes` darauf, dass Sie sich nicht gerade in einer laufenden X-Session befinden, wenn der Hostname neu gesetzt wird. Andernfalls kann ihre ⟨*DISPLAY*⟩-Variable nicht korrekt ausgewertet werden und Sie können keine neuen Fenster mehr starten.

DHCLIENT_MODIFY_RESOLV_CONF="yes"
Darf der DHCP Client Ihre `/etc/resolv.conf` ändern? Die

Standardeinstellung ist yes. Setzen Sie hier no oder enthält ⟨*MODIFY_RESOLV_CONF_DYNAMICALLY*⟩ in /etc/sysconfig/network/config den Wert no, wird die Datei /etc/resolv.conf nicht angerührt.

DHCLIENT_SET_DEFAULT_ROUTE="yes"
Soll der DHCP Client den Default Gateway bestimmen? Sollten mehrere dhcpcd Prozesse laufen, sollte dies nur einer von ihnen tun dürfen.

DHCLIENT_MODIFY_NTP_CONF="no"
Soll der DHCP Client die NTP Konfiguration (/etc/ntp.conf) verändern können?

DHCLIENT_MODIFY_NIS_CONF="no"
Soll der DHCP Client die NIS Konfiguration (/etc/yp.conf) verändern können?

DHCLIENT_SET_DOMAINNAME="yes"
Soll der DHCP Client den NIS Domain Namen setzen? (Nur sinnvoll, wenn der Server die nis-domain Option anbietet.)

DHCLIENT_KEEP_SEARCHLIST="no"
Soll der DHCP Client, wenn er eine neue /etc/resolv.conf schreibt, die bereits existierende Domain-Suchliste beibehalten und zu derjenigen hinzufügen, die er vom DHCP Server erhält?

DHCLIENT_LEASE_TIME=""
Hier können Sie (in Sekunden) angeben, für welchen Zeitraum der DHCP Server dem Client eine dynamische IP überlässt („least").

DHCLIENT_TIMEOUT="999999"
Sie können einen „Timeout" setzen, nach dem der Client automatisch abbricht, wenn er keine Antwort vom Server bekommt. Diese Einstellung betrifft nur dhcpcd.

DHCLIENT_REBOOT_TIMEOUT=""
Diese Option legt fest, wie lang dhcpcd versucht einen früheren „Lease" wiederzubekommen (im Init-Reboot-Zustand), bevor ein neuer „Lease" verwendet wird.

DHCLIENT_HOSTNAME_OPTION="AUTO"
Sie können einen bestimmten Hostnamen festlegen, den dhcpcd für DHCP Messages verwendet. Die Voreinstellung AUTO bewirkt, dass automatisch der Hostname gesendet wird.

DHCLIENT_CLIENT_ID=""
Hier legen Sie eine Zeichenkette fest, die als Client-ID gesendet wird. Nehmen Sie hier keinen Eintrag vor, wird die Hardware-Adresse der Netzwerkkarte gesendet.

DHCLIENT_VENDOR_CLASS_ID=""
Legt den „Vendor Class Identifier“ fest.

DHCLIENT_RELEASE_BEFORE_QUIT="no"
Soll der Client den Server benachrichtigen, wenn er eine Adresse nicht mehr benötigt, so dass diese wieder zum allgemeinen Gebrauch freigegeben werden kann? Diese Option unterstützt nur dhcpcd.

DHCLIENT_SLEEP="0"
Manche Interfaces brauchen eine bestimmte Zeit, bis sie korrekt initialisiert werden. Sie können hier eine Latenzzeit in Sekunden angeben, während der der DHCP Client die Initialisierung abwartet. Allerdings sollten solche Einstellungen separat für die einzelnen Interfaces vorgenommen werden.

network/ifcfg-eth0 Konfiguration der ersten Netzwerkkarte. Die folgenden Einstellungen lassen sich komfortabel mit YaST2 vornehmen.

STARTMODE=""
Wann wird das Interface aktiviert? `onboot` besagt, dass das Interface zur Bootzeit gestartet wird, `manual`, dass ifup manuell gestartet werden muss und `hotplug` ermöglicht die Aktivierung per Hotplug oder PCMCIA.

BOOTPROTO=""
Wählen Sie zwischen statische IP-Konfiguration oder dynamischer Adressvergabe mit DHCP (`dhcp`).

IPADDR=""
Hier tragen Sie die IP-Adresse für die erste Netzwerkkarte ein.

NETMASK=""
Hier tragen Sie die Netzmaske Ihres Netzes ein.

BROADCAST=""
Geben Sie die Broadcastadresse für Ihr Netzwerk an.

PREFIXLEN=""
Geben Sie die Länge des Prefix an.

NETWORK=""
Die Adresse Ihres Netzwerks.

network/ifcfg-lo Die Konfiguration des Loopback-Device.

network/wireless Die Konfiguration für Wireless LAN. Bitte verwenden Sie YaST2 zur Konfiguration.

news Einstellungen für den Zugriff auf den NNTP-Server.

ORGANIZATION=""
Der hier eingetragene Text erscheint in jedem News-Posting, das von dem betreffenden Rechner abgeschickt wird. Beispiel:
`Duesentrieb, Entenhausen`

NNTPSERVER="news"
Die Adresse des News-Servers; beziehen Sie Ihre News per UUCP und werden diese lokal gespeichert, sollten Sie hier `localhost` eintragen.

nfs NFS-Server. Gleichzeitig werden die Daemonen rpc.nfsd und rpc.mountd gestartet. Für eine weitergehende Beschreibung eines NFS-Servers (zum Beispiel die Festlegung der zu exportierenden Verzeichnisse) lesen Sie bitte Abschnitt *NFS – verteilte Dateisysteme* auf Seite 312.

REEXPORT_NFS="no"
Setzen Sie die Variable auf `yes`, um gemountete NFS-Verzeichnisse oder NetWare-Volumes zu re-exportieren.

onlineupdate Einstellungen für YaST2-Online-Update.

YAST2_LOADFTPSERVER="yes"
Beim Starten von YOU („YaST2-Online-Update“) die Liste der FTP-Server mit wget von `http://www.suse.de` aktualisieren. Diese Liste wird in `/etc/suseservers` eingetragen. Diese Variable ist auf `no` zu setzen, wenn die Liste nicht aktualisiert werden soll.

PROXY_USER=""
Benutzer des verwendeten Proxy.

PROXY_PASSWORD=""
Passwort für den verwendeten Proxy.

pcmcia PCMCIA-System/PC-Cards.

PCMCIA_SYSTEM="kernel"
Wählen Sie eines der beiden PCMCIA-Systeme aus: `external` oder `kernel`. Wenn nur eines der beiden Systeme installiert ist, wird der Inhalt dieser Variable ignoriert.

PCMCIA_PCIC=""
Dient der Festlegung des Socket-Treibers (Chipsets); gültige Werte sind `i82365` oder `tcic`, wenn das „externe“ PCMCIA-System verwendet wird (vgl. ⟨*PCMCIA_SYSTEM*⟩) und `yenta_socket`, `i82365` oder `tcic` bei Verwendung des Systems `Kernel`. Wenn die Variable leer ist (""), versucht das Skript selbstständig den richtigen Treiber herauszufinden; die Variable muss also nur gesetzt werden, wenn die automatische Erkennungen fehlschlägt.

PCMCIA_PCIC_OPTS=""
Festlegung der Sockettreiber-Timingparameter. Sie finden eine nähere Beschreibung unter `man i82365` oder `man tcic` und im PCMCIA-HOWTO (`/usr/share/doc/packages/pcmcia`) unter „PCIC_OPTS".

PCMCIA_CORE_OPTS=""
Hier legen Sie die „pcmcia_core" Optionen fest. Eine Beschreibung finden Sie unter `/usr/share/doc/packages/pcmcia` bei „CORE_OPTS". Diese Optionen sind für beide PCMCIA-Typen gültig.

postfix Die Konfiguration der Postfix Variablen. Benutzen Sie hierfür bitte das `mail` Modul von YaST2.

postgresql PostgreSQL.

POSTGRES_DATADIR="~postgres/data"
In welchem Verzeichnis soll die PostgreSQL Datenbank zu finden sein?

POSTGRES_OPTIONS=""
Die hier spezifizierten Optionen werden dem „PostgreSQL Master Daemon" beim Start übergeben. Bitte informieren Sie sich über Details auf den Manpages für `postmaster` und `postgresql`. Bitte verwenden Sie die Option `-D datadir` an dieser Stelle nicht; das Startup-Skript setzt diesen Wert ausgehend von ⟨*POSTGRES_DATADIR*⟩.

powermanagement apmd.

APMD_WARN_LEVEL="10"
Wollen Sie gewarnt werden, sobald die Batteriekapazität ein bestimmtes Niveau (Angabe in Prozent) unterschreitet? Die Standardeinstellung ist `10`; mit `0` deaktivieren Sie diese und die drei folgenden Optionen. Mehr zu apmd unter `man 8 apmd` oder im zugehörigen Init-Skript `/etc/init.d/apmd`.

APMD_WARN_ALL="no"
Sollen die apmd-Warnungen an alle Terminals gesendet werden? Dann wählen Sie `yes`, andernfalls werden sie in der Syslog-Datei erfasst. Die Standardeinstellung ist `no`.

APMD_WARN_STEP="0"
Die Warnmeldungen werden wiederholt, sobald die maximale Batteriekapazität um eine bestimmte Größe (⟨*APMD_WARN_STEP*⟩) abnimmt. `0` deaktiviert diese Einstellung.

APMD_CHECK_TIME="0"
apmd überprüft standardmässig den Batteriestatus, wann immer es vom BIOS ein Event gemeldet bekommt. Soll diese Überprüfung öfter stattfinden, setzen Sie den Wert dieser Variable auf einen Wert größer

als 0 Sekunden. Allerdings wird Ihre Festplatte dann bei jeder Überprüfung wieder angefahren. Die Standardeinstellung ist `0`.

APMD_DEBUG="no"
apmd und das apmd_proxy Skript können „gesprächiger“ gemacht werden. Bei `yes` werden Sie darüber informiert, wann und wie apmd_proxy aufgerufen wird. Wenn Sie alles sehen wollen, was innerhalb von apmd_proxy auf `stdout` und `stderr` ausgegeben wird, wählen Sie `error`. Mit `all` entgeht Ihnen nichts. Standardeinstellung ist `no`.

APMD_ADJUST_DISK_PERF="no"
Um Energie zu sparen, sollte Ihre Festplatte nach einer bestimmten „Idle Time“ heruntergefahren werden. Wenn Sie allerdings Prozesse betreiben, die in regelmäßigen Abständen und häufig auf die Platte schreiben, wird diese Option wenig ausrichten. Per Voreinstellung ist diese Option inaktiv.

APMD_BATTERY_DISK_TIMEOUT="12"
Setzen Sie den „Timeout“ fest, nach dem die Festplatte heruntergefahren werden soll. Allerdings bemisst sich der Wert dieser Variable nicht in Minuten oder Sekunden. Bitte lesen Sie für Details die Manpage von hdparm. Natürlich macht diese Einstellung nur Sinn, wenn Sie zuvor ⟨*ADJUST_DISK_PERF*⟩ auf `yes` gesetzt haben.

APMD_AC_DISK_TIMEOUT="0"
Soll die Festplatte auch heruntergefahren werden, wenn der Rechner am Stromnetz hängt? Wenn ja, wann (siehe oben)? Diese Option ist per Voreinstellung inaktiv.

APMD_BATTERY_LOW_SHUTDOWN="0"
Manche Laptop BIOSe senden nach Unterschreiten einer bestimmten Batteriekapazität eine „battery low“ Meldung. Ihr System kann automatisch eine bestimmte Zeit nach diesem Ereignis heruntergefahren werden. Geben Sie einen Wert in Minuten an. `1` ist das Minimum, `0` deaktiviert dieses Verhalten.

APMD_SET_CLOCK_ON_RESUME="no"
Sollten Ihre Zeiteinstellungen nach einem Standby oder Suspend aus dem Tritt geraten, setzen Sie diese Variable auf `yes`. Dann wird die Kernelzeit automatisch auf den Wert gesetzt, der in der GMT-Variable gesetzt wurde. Diese Option ist per Voreinstellung inaktiv.

APMD_SUSPEND_ON_AC="yes"
Ihr System wird auch dann heruntergefahren, wenn es an das Stromnetz angeschlossen ist. Mit `no` schalten Sie dieses Verhalten ab.

APMD_PCMCIA_SUSPEND_ON_SUSPEND="no"
Sollte Ihr PCMCIA keine APM-Unterstützung bieten, veranlassen Sie apmd dazu, Ihre Karten vor dem Suspend des Gesamtsystems in den Suspend-Modus zu bringen.

APMD_PCMCIA_EJECT_ON_SUSPEND="no"
Manche PCMCIA-Karten (insbesondere SCSI-Karten) reagieren nicht angemessen auf ein Suspend-Ereignis. Deshalb kann es notwendig werden, sie per `cardctl eject` zu deaktivieren.

APMD_INTERFACES_TO_STOP=""
Sollte das Setup Ihrer integrierten Netzwerkkarte mit dem Suspend/Resume-Zyklus nicht richtig zurechtkommen, setzen Sie hier den Interface Namen. Das angegebene Interface wird jetzt bei einem Suspend korrekt heruntergefahren und wieder hochgefahren, sobald der Suspend-Modus aufgehoben wird.

APMD_INTERFACES_TO_UNLOAD=""
Sollte Ihr Netzwerk-Interface auch nach Auswertung von ⟨*APMD_INTERFACES_TO_STOP*⟩ nicht korrekt heruntergefahren werden können, tragen Sie hier das Treibermodul Ihres Netzwerk-Interfaces ein. Es wird dann beim Suspend aus dem Speicher geladen und bei einem Resume wieder eingelesen.

APMD_LEAVE_X_BEFORE_SUSPEND="no"
Abhängig von Ihrer Grafikkarte kann die Rückkehr in den Grafikmodus nach dem Suspend nicht korrekt funktionieren. Sie können vor dem Suspend auf die Textkonsole wechseln und nach dem Resume wieder auf die X-Console zurückkehren. Die Standardeinstellung ist `0`.

APMD_LEAVE_X_BEFORE_STANDBY="no"
Siehe ⟨*APMD_LEAVE_X_BEFORE_SUSPEND*⟩. Auch die Rückkehr nach einem Standby kann erschwert sein. Die Standardeinstellung ist `0`.

APMD_LOCK_X_ON_SUSPEND="no"
Soll apmd Ihr Display „locken“? Wenn nur ein X-Server auf Ihrem System läuft und niemand über ein virtuelles Terminal Zugriff auf Ihr System hat, kann dieser Zustand als „sicher“ angesehen werden. Zusätzlich bietet eine verschlüsselte Datenpartition einen sehr guten Schutz, wenn Ihr Laptop gestohlen werden sollte. Die Standardeinstellung ist `0`.

APMD_STOP_SOUND_BEFORE_SUSPEND="no"
Auch Soundmodule überleben unter Ümständen einen Suspend/Resume-Zyklus nicht. Sie können hier die Soundmodule angeben, die vor dem Suspend aus dem Speicher entfernt werden sollen und bei einem Resume wieder geladen werden. Vor dem Suspend schließen Sie bitte alle Soundapplikationen. Je nach verwendetem Soundsystem weisen Sie dieser Variable die Werte `alsa`, `oss` oder

kernel zu. Mit no wird kein „Unload" der Soundmodule durchgeführt.

APMD_KBD_RATE=""
Unter Umständen muss auch die Tastaturwiederholungsrate und -verzögerung wieder neu gesetzt werden. Tragen Sie einen möglichen numerischen Wert ein oder lassen Sie diese beiden Variablen leer, wenn Sie dieses Verhalten nicht wünschen.

APMD_KBD_DELAY=""

APMD_TURN_OFF_IDEDMA_BEFORE_SUSPEND=""
Manche Notebooks kehren nicht korrekt in den normalen Betriebsmodus zurück, wenn die Festplatte zuvor im DMA-Modus war. Tragen Sie alle Platten hier ein, die einen Stop des DMA-Modus benötigen, um in den normalen Betriebsmodus zurückzukehren.

printer Drucker.

DEFAULT_PRINTER="lp"
Name des Standarddruckers, wenn beim lpr-Aufruf kein Drucker mit -P angegeben ist.

proxy Proxy-Einstellungen.

HTTP_PROXY=""
Einige Programme (z. B. lynx, arena oder wget) können Proxy-Server benutzen, wenn diese Umgebungsvariable entsprechend gesetzt ist; SuSEconfig kann diese in /etc/SuSEconfig/* setzen (vgl. in der SDB file:/usr/share/doc/sdb/de/html/lynx_proxy.html). Beispiel: "http://proxy.provider.de:3128/" .

FTP_PROXY=""
Proxy für FTP. Beispiel: "http://proxy.provider.de:3128/" .

NO_PROXY="localhost"
Mittels dieser Variable lassen sich (Sub-)Domains vom Proxy ausschließen. Beispiel: "www.me.de, do.main, localhost" .

security Einstellungen zur Systemsicherheit.

CHECK_PERMISSIONS="set"
Legt fest, ob die Datei-Rechte anhand der Datei /etc/permissions überprüft werden sollen. Mit set werden falsche Einstellungen berichtigt, mit warn werden nur „Warnungen" hergestellt, no wird dieses Merkmal abgestellt.

PERMISSION_SECURITY="easy local"
In /etc/permissions.paranoid, /etc/permissions.secure und /etc/permissions.easy sind drei Sicherheitsstufen vorbereitet. Tragen Sie hier easy, secure oder paranoid ein; eigene Einstellungen können Sie z. B. in /etc/permissions.local vornehmen und dann die Erweiterung local als Wert hinzufügen.

Beachten Sie, dass bei Auswahl der Option paranoid einige Systemdienste möglicherweise nicht mehr so zur Verfügung stehen, wie Sie das wünschen; dies bedeutet, dass Sie gezielt die Dienste „freischalten" müssen, die Sie benötigen!

Achtung: Wenn Sie Angaben in /etc/permissions.local vornehmen, kontrollieren Sie bitte, dass diese in keinem Konflikt zu Vorgaben des Rotationsmechnismus (Paket logrotate) stehen. logrotate überschreibt Angaben von /etc/permissions.local; vgl. Abschnitt *Protokoll-Dateien – das Paket logrotate* auf Seite 198.

sendmail Die sendmail-Variablen; verwenden Sie das mail-Modul von YaST2 zur Konfiguration.

sound Angaben zur Soundkonfiguration

LOAD_SEQUENCER="yes"
Sollen die ALSA Sequencer Module beim Boot-up geladen werden? Diese Module benötigen Sie nur, wenn Sie mit MIDI Devices arbeiten. Sollten Sie kein MIDI benötigen, deaktivieren Sie diese Option. Die Module können auch automatisch nachgeladen werden.

ssh „Secure Shell Daemon"; stellen Sie vor dem Starten sicher, dass ein „host key" existiert – vgl. dazu die Dokumentation unter /usr/share/doc/packages/ssh sowie die Manual-Pages.

SSHD_OPTS=""

suseconfig Grundeinstellungen für SuSEconfig.

ENABLE_SUSECONFIG="yes"
Legt fest, ob SuSEconfig die Konfiguration durchführen soll. Bitte auf keinen Fall ausschalten, falls Sie Installationssupport in Anspruch nehmen wollen.

MAIL_REPORTS_TO="root"
Festlegen, an wen SuSEconfig Berichte per E-Mail schicken soll, die während der automatischen System-Administration erzeugt werden.

MAIL_LEVEL="warn"
Zwei Stufen sind möglich: bei warn werden nur die wichtigen Meldungen verschickt; bei all auch die Protokoll-Dateien („Logs").

CREATE_INFO_DIR="yes"
Legt fest, ob automatisch die Datei `/usr/share/info/dir` mit einem Perl-Skript erstellt werden soll, die einen Index für alle vorhandenen Info-Seiten bildet.

CHECK_ETC_HOSTS="yes"
Legt fest, ob SuSEconfig die Datei `/etc/hosts` überprüfen und ggf. ändern soll.

BEAUTIFY_ETC_HOSTS="no"
Falls `/etc/hosts` sortiert werden soll.

SORT_PASSWD_BY_UID="no"
`/etc/passwd` und `/etc/group` nach „UID" bzw. „GID" sortieren.

CWD_IN_ROOT_PATH="no"
Aktuelles Verzeichnis (engl. *current working directory*) im Pfad von `root`; davon wird aus Sicherheitsgründen abgeraten. Diese Einstellung betrifft alle Benutzer mit einer UID unter 100 (engl. *system users*).

CWD_IN_USER_PATH="yes"
Soll das aktuelle Verzeichnis (engl. *current working directory*) im Pfad der normalen Benutzer liegen?

CREATE_PERLLOCAL_POD="yes"
`yes` erlaubt es SuSEconfig, die Datei `perllocal.pod` zu verändern. In `perllocal.pod` sind die Installationsspezifika einzelner Perl-Module enthalten.

UPDATE_GROFF_CONF="yes"
`DESC` aktualisieren, um die Blattgröße korrekt einzustellen.

GROFF_PAGESIZE=""
Wenn die Blattgröße aus der `/etc/printcap` nicht hervorgeht, ist die Einstellung hier vorzunehmen. `letter`, `legal`, `a4` und `a5` werden von groff und ghostscript unterstützt.

sysctl System auf Kernellevel kontrollieren.

IP_DYNIP="no"
Den „dynamic IP patch" beim Booten aktivieren; bei `yes` gibt das Skript `/etc/init.d/boot.proc` diesen Patch durch einen Eintrag in das `/proc`-Dateisystem frei.

IP_TCP_SYNCOOKIES="yes"
Schutz vor „Syn Flooding" (engl. *syn flood protection*) aktivieren; vgl. `/usr/src/linux/Documentation/Configure.help`.

IP_FORWARD="no"
Wenn der Rechner über zwei Netzwerk-Interfaces weiterleiten soll, ist ⟨*IP_FORWARD*⟩ auf `yes` zu setzen; dies ist bei einem „Router" der Fall.

ENABLE_SYSRQ="no"
Interna des Kernels betrachten. Vor Anwendungen bitte unbedingt /usr/src/linux/Documentation/sysrq.txt lesen!

DISABLE_ECN="yes"
Mit yes wird ECN (engl. *early congestion notification*) zur Bootzeit abgeschaltet; nützlich wenn es Verbindungsschwierigkeiten zur anderen Rechnern im Internet gibt, die aufgrund einer eigenartigen Firewallkonfiguration Netzwerkpakete verwerfen und diese Verbindungen zuvor mit dem Linux-Kernel 2.2 funktioniert hatten.

BOOT_SPLASH="yes"
Den „Splashscreen“ zur Bootzeit abschalten.

syslog Syslog-Daemon konfigurieren.

KERNEL_LOGLEVEL="/var/lib/dhcp/dev/log"
Zusätzlicher Eintrag, der vom dhcp-server Paket generiert wurde. Der hier eingetragene Dateiname wird mittels -a <Dateiname> als zusätzlicher Socket über ⟨*SYSLOGD_PARAMS*⟩ automatisch hinzugefügt, sobald syslogd gestartet wird. Dies ist nötig, um einem „chrooted“ betriebenen dhcpd nach einem Neustart des syslogd weiteres Logging zu ermöglichen.

KERNEL_LOGLEVEL="1"
Loglevel für klogd.

SYSLOGD_PARAMS=""
Parameter für den syslogd; z. B. "-r -s my.dom.ain".

syslog-ng Syslog-ng konfigurieren.

SYSLOG_NG_REPLACE="yes"
Soll syslog-ng den „alten“ syslogd ersetzen? Wird diese Variable auf no gesetzt, starten beide Programme.

SYSLOG_NG_PARAMS=""
Parameterübergabe an syslog-ng. Bitte entnehmen Sie man 8 syslog-ng die nötigen Details.

tetex TeX/LaTeX.

CLEAR_TEXMF_FONTS="no"
Im Rahmen der automatischen Fontgenerierung für das TeX/LaTex-System werden Bitmap-Fonts im Verzeichnis /var/cache/fonts/ abgelegt. Setzen Sie diese Variable auf yes werden in diesem Verzeichnis regelmäßig alle Fonts gelöscht, die länger als 20 Tage nicht verwendet wurden.

windowmanager Windowmanager.

DEFAULT_WM="kde"
Mögliche Einstellungen: kde, gnome, fvwm etc.

INSTALL_DESKTOP_EXTENSIONS="yes"
SuSE-Erweiterungen für neu angelegte Benutzer installieren. Dabei handelt es sich um „Themes“ und zusätzliche Funktionen, die das System benutzerfreundlich gestalten.

KDE_USE_FAM="no"
fam-Daemon vorwenden; nur sinnvoll bei Verzeichnissen, die über NFS eingehängt werden.

KDE_USE_FAST_MALLOC="yes"
Das verbesserte malloc verwenden.

SUSEWM_UPDATE="yes"
Legt fest, ob SuSEconfig die systemweiten Konfigurationsdateien für die Windowmanager in Abhängigkeit von den installierten Software-Paketen anpassen soll.

SUSEWM_WM="all"
Liste der Windowmanager, für die Konfigurationsdateien erzeugt werden sollen; mögliche Werte: fvwm, fvwm2, fvwm95, bowman, mwm, ctwm, kwm sowie all (für alle).

SUSEWM_XPM="yes"
Das Paket 3dpixms muss installiert sein, damit beim fvwm/fvwm95 Pixmaps in den Menüs erscheinen; wenn der Windowmanager dadurch für den Benutzer zu langsam wird, ist diese Variable auf no zu setzen.

xdmsc Zum Betrieb von X-Terminals.

START_RX="no"
Bevor Sie diese Variable verändern, editieren Sie bitte zuerst die Datei /etc/inittab und entfernen Sie dort die Zeile mit /sbin/init.d/rx. Ausserdem müssen die Variablen ⟨*RX_XDMCP*⟩ und ⟨*RX_RHOST*⟩ gesetzt. Dann setzen Sie diese Variable auf yes, um ein X-Terminal zu bekommen.

RX_XDMCP="broadcast"
Konfiguration der XDMCP (engl. *XDM Control Protocol*) Requests. query – bei einem XDM-Server um ein Login-Fenster anfragen, indirect – bei einem XDM-Server um ein Chooser-Menü anfragen und broadcast – bei allen im Netz befindlichen XDM-Servern um ein Login-Fenster anfragen, der Erste gewinnt. Für die beiden Optionen query und indirect muss ⟨*RX_HOST*⟩ gesetzt sein.

RX_RHOST=""
Name des XDM-Hosts.

RX_DSP=""
Hier können Sie optional die Displaynummer festlegen. Die Standardeinstellung ist `:0`.

RX_BPP=""
Farbtiefe des lokalen X-Servers. Diese Angabe ist optional.

RX_CLASS=""

xntp Startet den „Network Time Protocol (NTP) Daemon“ aus dem Paket `xntp`; die Konfiguration selbst geschieht über die Datei `/etc/ntp.conf`.

XNTPD_INITIAL_NTPDATE="AUTO-2"
Mit Leerzeichen abgeteilte Liste der NTP-Server, von denen die Zeit geholt werden kann, bevor der lokale Server gestartet wird; z. B. "`sonne.kosmos.all` ".

Es ist auch möglich `AUTO` einzutragen, dann werden alle Server und Peers abgefragt, die in `/etc/ntpd.conf` konfiguriert sind. Zudem kann man die Gesamtzahl der abzufragenden Server durch anhängen einer Zahl einschränken; Vorgabe ist `AUTO-2`.

Funkuhren haben Adressen in der Form `127.127.T.U`; dabei steht `T` für den Typ der Uhr und `U` ist die „unit number“ im Bereich von `0` bis `3`. – Die meisten dieser Uhren benötigen eine serielle Schnittstelle oder einen speziellen Bus. Die dafür vorgesehene Gerätedatei (Device) wird normalerweise durch einen symbolischen Link `/dev/device-U` auf die tatsächliche Hardware angegeben; dabei hat `U` mit der zuvor erwähnten „unit number“ übereinzustimmen. Vgl. auch `/usr/share/doc/packages/xntp/html/refclock.htm`.

Beispiel: Wer eine Funkuhr hat, die an eine serielle Schnittstelle angeschlossen ist, der benötigt auch einen entsprechenden Symlink. Wie der zu heißen hat, erfährt man über `refclock.htm`. – Für die üblichen DCF77-Empfänger, ist der „PARSE“-Treiber zuständig:

```
## Type 8 Generic Reference Driver (PARSE)
## Address:     127.127.8.u
## Serial Port: /dev/refclock-u
```

Wer also über einen `ntp.conf`-Eintrag den `server 127.127.8.0` wählt, der braucht auch einen Symlink von `/dev/refclock-0` auf `ttySx` – dabei steht `x` für die Schnittstelle, an die die Funkuhr angeschlossen ist.

ypbind Konfiguration eines NIS-Client. Zusätzliche Informationen: Der Domainname steht direkt in `/etc/defaultdomain`. Server wird bei der Konfiguration mit YaST2 direkt in `/etc/yp.conf` eingetragen; vgl. Abschnitt *NIS – Network Information Service* auf Seite 307.

YPBIND_OPTIONS=""
Optionen.

YPBIND_LOCAL_ONLY="no"
Setzen Sie diese Option auf `yes`, verbindet sich ypbind nur mit dem lokalen Loopback Interface. Andere Hosts können es nicht abfragen.

YPBIND_BROADCAST="no"
Wird diese Option auf `yes` gesetzt, ignoriert ypbind die Datei `/etc/yp.conf` und versucht, über einen Broadcast-Call einen verfügbaren NIS-Server im lokalen Subnetz zu finden. Bitte vermeiden Sie diese Option, da sie ein großes Sicherheitsloch darstellt.

YPBIND_BROKEN_SERVER="no"
Sollten Sie in Ihrem Netz einen NIS-Server haben, der sich nur mit höheren Ports als 1024 verbindet, ist diese Option auf `yes` zu setzen. Allerdings stellt dies ein Sicherheitsrisiko dar – Sie sollten die Verwendung einer anderen NIS-Server Implementation in Betracht ziehen.

ypserv Einstellungen zur Konfiguration eines NIS-Servers

YPPWD_SRCDIR="/etc"
Falls Sie ein von `/etc` abweichendes Verzeichnis für die Quelldateien für `passwd`, `shadow` und `group` festlegen wollen, geben Sie es hier an.

YPPWD_CHFN="no"
Darf der Benutzer mittels ypchfn sein GECOS-Feld (mit zusätzlichen Informationen wie Telefonnummern etc.) ändern?

YPPWD_CHSH="no"
Darf der Benutzer mittels ypchsh sein Standard-Login ändern?

zope Konfiguration eines ZOPE-Systems.

ZOPE_FTP="yes"
Soll Zope einen FTP-Zugang bieten?

ZOPE_FTP_PORT="8021"
Über welchen Port soll der Zugang möglich sein?

ZOPE_HTTP_PORT="8080"
Falls Zope als Standalone Webserver fungieren soll, müssen Sie den Port festlegen, den er belegen soll.

Teil IV

Netzwerk

Grundlagen der Vernetzung

Linux, ein wahres Kind des Internets, bietet Ihnen alle Voraussetzungen und notwendigen Netzwerktools zur Einbindung in diverse Netzwerkstrukturen. Im folgenden erhalten Sie eine Einführung in das normalerweise von Linux verwendete Protokoll TCP/IP, dessen Dienstleistungen und auch besonderen Eigenschaften. Anschließend zeigen wir Ihnen die Einrichtung eines Netzwerkzugangs mit einer Netzwerkkarte unter SuSE Linux mit Hilfe von YaST2. Es werden die zentralen Konfigurationsdateien besprochen und einige der wichtigsten Tools aufgeführt.

Da die Konfiguration eines Netzwerks beliebig komplex sein kann, werden in diesem Kapitel nur die grundlegenden Mechanismen dargestellt. Auch die Internet-Anbindung per PPP via Modem, ISDN oder DSL lässt sich mit YaST2 bequem konfigurieren und ist im *Benutzer-Handbuch* erklärt.

TCP/IP - Das von Linux verwendete Protokoll 270
IPv6 – Internet der nächsten Generation 278
Die Einbindung ins Netzwerk 284
Manuelle Netzwerkkonfiguration 287
Routing unter SuSE Linux 296
DNS – Domain Name Service 297
NIS – Network Information Service 307
NFS – verteilte Dateisysteme 312
DHCP 317

TCP/IP - Das von Linux verwendete Protokoll

Linux und andere Unix-Betriebssysteme verwenden das TCP/IP-Protokoll. Genau genommen handelt es sich um eine Protokollfamilie, die ganz unterschiedliche Dienstleistungen bietet. TCP/IP wurde aus einer militärischen Anwendung heraus entwickelt und in der heute verwendeten Form ca. 1981 in einem so genannten RFC festgelegt. Bei RFC (engl. *Request for comments*) handelt es sich um Dokumente, die die verschiedenen Internetprotokolle und die Vorgehensweise bei der Implementierung des Betriebssystems und von Applikationen beschreiben. Auf diese RFC-Dokumente können Sie direkt über das Web zugreifen, die URL lautet `http://www.ietf.org/`. In der Zwischenzeit sind einige Verfeinerungen am TCP/IP Protokoll vorgenommen worden, am grundlegenden Protokoll hat sich seit 1981 aber nichts geändert.

Tipp

Die RFC Dokumente beschreiben den Aufbau der Internet Protokolle. Falls Sie Ihr Know-how über ein bestimmtes Protokoll vertiefen wollen, ist das passende RFC Dokument die richtige Anlaufstelle:

`http://www.ietf.org/rfc.html`

Tipp

Die in Tabelle 12.1 auf der nächsten Seite genannten Dienste stehen zur Verfügung, um Daten zwischen zwei Linuxrechnern über TCP/IP auszutauschen:

Protokoll	Beschreibung
TCP	(engl. *Transmission control protocol*) Ein verbindungsorientiertes, gesichertes Protokoll. Die zu übertragenden Daten werden aus der Sicht der Applikation als Datenstrom verschickt und vom Betriebssystem selbst in das passende Übertragungsformat gebracht. Die Daten kommen bei der Zielapplikation auf dem Zielrechner als exakt der Datenstrom an, als der sie abgeschickt wurden. TCP stellt sicher, dass unterwegs keine Daten verloren gehen und nichts durcheinander kommt. TCP wird dort verwendet, wo die Reihenfolge der Daten wichtig ist und der Begriff Verbindung Sinn macht.

Tabelle 12.1: *Fortsetzung auf der nächsten Seite…*

UDP	(engl. *User Datagram protocol*) Ein verbindungsloses, ungesichertes Protokoll. Die zu übertragenden Daten werden paketorientiert verschickt, die Datenpakete werden dabei schon von der Applikation erzeugt. Die Reihenfolge der Daten beim Empfänger ist nicht garantiert, ebenso kann es passieren, dass einzelne Datenpakete verloren gehen. UDP eignet sich für datensatzorientierte Applikationen und bietet kleinere Latenzzeiten als TCP.
ICMP	(engl. *Internet control message protocol*) Im Wesentlichen ist das kein für den Benutzer verwendbares Protokoll, sondern ein spezielles Steuerprotokoll, das Fehlerzustände übermittelt und das Verhalten der an der TCP/IP-Datenübertragung beteiligten Rechner steuern kann. Zusätzlich wird durch ICMP noch ein spezieller Echo-Modus bereitgestellt, den man mit dem Programm ping prüfen kann.
IGMP	(engl. *Internet group management protocol*) Dieses Protokoll steuert das Verhalten von Rechnern bei der Verwendung von IP-Multicast. Leider kann IP-Multicasting in diesem Rahmen nicht vorgestellt werden.

Tabelle 12.1: *Verschiedene Protokolle der TCP/IP Protokollfamilie*

Fast alle Hardwareprotokolle arbeiten paketorientiert. Die zu übertragenden Daten müssen in kleine „Päckchen“ gepackt werden und können nicht „in einem Rutsch“ verschickt werden. Deshalb arbeitet auch TCP/IP mit kleinen Datenpaketen. Die Maximalgröße eines TCP/IP Paketes ist knapp 64 Kilobyte. In der Praxis sind die Pakete normalerweise viel kleiner, da die Netzwerkhardware der limitierende Faktor ist. So ist die zulässige Maximalgröße eines Datenpaketes auf dem Ethernet ca. 1500 Byte. Dementsprechend wird die Paketgröße des TCP/IP Pakets begrenzt, wenn die Daten über ein Ethernet geschickt werden. Will man mehr Daten übertragen, müssen vom Betriebssystem entsprechend mehr Datenpakete verschickt werden.

Schichtenmodell

Über IP (engl. *Internet protocol*) findet eine ungesicherte Datenübertragung statt. TCP (engl. *Transmission control protocol*) ist gewissermaßen nur ein Aufsatz auf das darunter liegende IP, um eine gesicherte Übertragung der Daten

zu garantieren. IP selbst ist wiederum ein Aufsatz auf das darunter liegende, hardwareabhängige Protokoll, zum Beispiel Ethernet. Kenner sprechen hier vom „Schichtenmodell“. Vergleichen Sie hierzu die Abbildung 12.1.

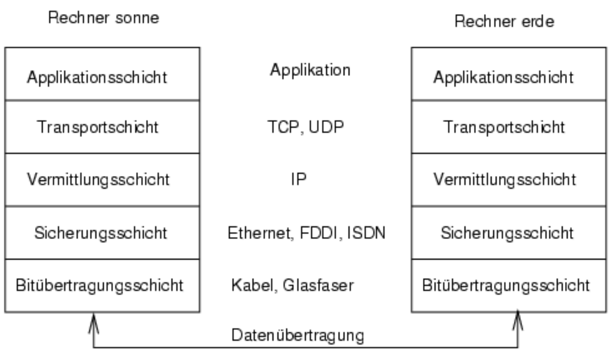


Abbildung 12.1: *Vereinfachtes Schichtenmodell für TCP/IP*

In der Abbildung sind jeweils ein oder zwei Beispiele für die jeweilige Schicht erwähnt. Wie Sie sehen, sind die Schichten nach „Abstraktionsebenen“ geordnet, die unterste Schicht ist sehr nah an der Hardware. Die oberste Schicht hingegen abstrahiert die darunter liegende Hardware nahezu vollständig. Jede der Schichten hat eine ganz spezielle Funktion, die zum Großteil schon aus der Bezeichnung hervorgeht. So wird das verwendete Netzwerk (z. B. Ethernet) durch die Bitübertragungsschicht und die Sicherungsschicht verkörpert.

- Während sich Schicht 1 mit solchen Dingen wie Kabeltypen, Signalformen, Signalkodierung und ähnlichem beschäftigt ist Schicht 2 für das Zugriffsverfahren (Welcher Rechner darf wann Daten schicken?) und eine Fehlerkorrektur (Datensicherung - deshalb `Sicherungsschicht`) zuständig. Die Schicht 1 nennt man die `Bitübertragungsschicht`.
- Schicht 3 wiederum, die `Vermittlungsschicht` ist für die Datenübertragung über weite Strecken verantwortlich. Die Vermittlungsschicht stellt sicher, dass die Daten auch über weite Strecken beim richtigen Empfänger ankommen und zugestellt werden können.
- Schicht 4, die `Transportschicht`, ist für die Daten der Applikation verantwortlich und stellt sicher, dass die Daten in der richtigen Reihenfolge ankommen und nicht verloren gehen. Die Sicherungsschicht ist nur dafür verantwortlich, dass die ankommenden Daten korrekt sind. Gegen das „Verlieren“ von Daten schützt die `Transportschicht`.

- Schicht 5 schließlich ist die Datenverarbeitung durch die Applikation selbst.

Damit jede der Schichten die ihr zugeteilte Aufgabe erfüllen kann, müssen zusätzliche Informationen der jeweiligen Schicht im Datenpaket im `Header`, dem Kopf des Datenpakets, gespeichert werden. Jede der Schichten fügt einen kleinen Datenblock, den sog. „Protokollkopf“ (engl. *Protocol header*), an das im Entstehen begriffene Paket vorne dran. Schauen wir uns also einmal ein beliebiges TCP/IP-Datenpaket an, das auf einem Ethernetkabel unterwegs ist, so setzt sich dieses wie in Bild 12.2 abgebildet zusammen.

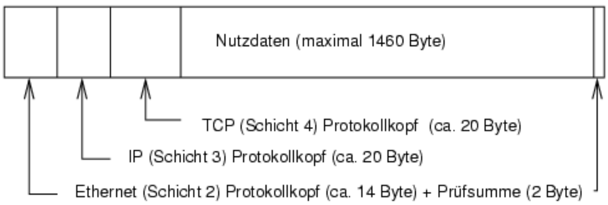


Abbildung 12.2: *TCP/IP Paket im Ethernet*

Wie Sie sehen, ist die Welt nicht perfekt und ohne Ausnahme. Die Prüfsumme der Sicherungsschicht befindet sich am Ende des Pakets und nicht am Anfang. Dies bringt aber für die Netzwerkhardware eine Vereinfachung. Die maximal mögliche Menge der Nutzdaten in einem Paket beträgt im Ethernet-Netzwerk 1460 Byte.

Möchte eine Applikation also Daten über das Netzwerk verschicken, durchlaufen die Daten die einzelnen Schichtebenen, die alle im Linuxkernel (Ausnahme Schicht 1: Netzwerkkarte) implementiert sind. Jede der Schichten ist dafür verantwortlich, die Daten so aufzubereiten, dass sie an die jeweils darunter liegende Schicht weitergereicht werden können. Die unterste Schicht ist schließlich für den eigentlichen Datenversand zuständig. Beim Empfang läuft das ganze nun umgekehrt ab. Wie bei den Schalen einer Zwiebel werden von jeder Schicht die Protokollköpfe von den Nutzdaten entfernt. Schicht 4 ist dann letztendlich dafür verantwortlich, die Daten für die Applikation auf dem Zielrechner bereitzustellen. Dabei kommuniziert eine Schicht immer nur mit der Schicht direkt über oder unter ihr. Für eine Applikation ist es also irrelevant, ob die Daten über ein 100-MBit/s-FDDI-Netzwerk oder über eine 56-KBit/s-Modemleitung übertragen werden. Umgekehrt ist es für die Datenübertragungsleitung egal, welche Daten eigentlich verschickt werden, solange sie richtig verpackt sind.

IP-Adresse (binär):	`11000000 10101000 00000000 00010100`
IP-Adresse (dezimal):	`192. 168. 0. 20`

Tabelle 12.2: *Schreibweise einer IP-Adresse*

IP-Adressen und Routing

IP-Adressen

Jeder Computer im Internet hat eine eindeutige 32-Bit-Adresse. Diese 32 Bit bzw. 4 Byte werden normalerweise wie in Tabelle 12.2 in der zweiten Zeile abgebildet geschrieben.

Die vier Bytes werden also im dezimalen Zahlensystem durch einen Punkt getrennt nebeneinander geschrieben. Die IP-Adresse ist einem Rechner bzw. einer Netzwerkschnittstelle zugeordnet, sie kann also nicht woanders auf der Welt nochmals verwendet werden. Ausnahmen von diesen Regeln gibt es zwar, spielen aber bei der folgenden Betrachtung erst einmal keine Rolle.

Auch die Ethernetkarte besitzt selbst eine eindeutige Adresse, die so genannte `MAC` (engl. *Media access control*) Adresse. Diese ist 48 Bit lang, weltweit eindeutig und wird vom Hersteller der Netzwerkkarte fest in der Hardware gespeichert. Durch die Vergabe der Adresse vom Hersteller ergibt sich aber ein fataler Nachteil: Die `MAC`-Adressen bilden kein hierarchisches System, sondern sind mehr oder weniger zufällig verteilt. Sie können daher nicht zur Adressierung eines weit entfernten Rechners verwendet werden. Die `MAC`-Adresse spielt aber bei der Kommunikation von Rechnern in einem lokalen Netz eine entscheidende Rolle (und ist der Hauptbestandteil des Protokollkopfes von Schicht 2).

Zurück zu den IP-Adressen: Die Punkte deuten schon an, dass die IP-Adressen ein hierarchisches System bilden. Bis Mitte der 90er Jahre waren die IP-Adressen fest in Klassen eingeteilt. Dieses System erwies sich aber als zu unflexibel und daher wurde diese Aufteilung aufgegeben. Man verwendet nun „klassenloses Routing“ (CIDR (engl. *classless inter domain routing*)).

Netzmasken und Routing

Da der Rechner mit der IP-Adresse `192.168.0.20` erst einmal nicht wissen kann, wo sich der Rechner mit der IP-Adresse `192.168.0.1` befindet, wurden die Netzmasken erdacht.

Vereinfacht gesagt definiert die (Sub-)Netzmaske auf einem Rechner mit IP-Adresse, was „drinnen“ und was „draußen“ ist. Rechner, die sich „drinnen“

IP-Adresse:192.168.0.20	11000000 10101000 00000000 00010100
Netzmaske: 255.255.255.0	11111111 11111111 11111111 00000000
Ergebnis binär	11000000 10101000 00000000 00000000
Ergebnis dezimal	192. 168. 0. 0
IP-Adresse: 213.95.15.200	11010101 10111111 00001111 11001000
Netzmaske: 255.255.255.0	11111111 11111111 11111111 00000000
Ergebnis binär	11010101 10111111 00001111 00000000
Ergebnis dezimal	213. 95. 15. 0

Tabelle 12.3: *Verknüpfung der IP-Adressen mit der Netzmaske*

(Profis sagen: „im gleichen Subnetz“) befinden, können direkt angesprochen werden. Rechner, die sich „draußen“ („nicht im gleichen Subnetz“) befinden, müssen über ein so genanntes Gateway oder Router angesprochen werden. Da jedes Netzwerkinterface eine eigene IP-Adresse bekommen kann, ahnen Sie schon, dass es schnell beliebig kompliziert wird.

Bevor ein Netzwerkpaket auf die Reise geschickt wird, läuft folgendes im Rechner ab: Die Zieladresse wird mit der Netzmaske bitweise UND verknüpft. Daraufhin wird auch die Absendeadresse bitweise mit der Netzmaske UND verknüpft (siehe Tabelle 12.3). Stehen mehrere Netzwerkinterfaces zur Verfügung, werden in der Regel alle möglichen Absendeadressen überprüft.

Die Ergebnisse der UND-Verknüpfungen werden verglichen. Ergibt sich zwischen den Ergebnissen eine exakte Übereinstimmung, so befindet sich der Zielrechner im gleichen Subnetz. Ansonsten muss er über ein Gateway angesprochen werden. Das heißt, je mehr „1“ Bits sich in der Netzmaske befinden, desto weniger Rechner können direkt, sondern nur über ein Gateway angesprochen werden. Zur Veranschaulichung sind in Tabelle 12.3 mehrere Beispiele aufgeführt.

Die Netzmaske wird wieder – wie schon die IP-Adresse – in Form von durch Punkte getrennten Dezimalzahlen geschrieben. Da die Netzmaske auch ein 32-Bit-Wert ist, werden vier Zahlenwerte nebeneinander geschrieben. Welche Rechner Gateway sind oder welche Adressbereiche über welche Netzwerkschnittstelle erreichbar sind, muss vom Benutzer konfiguriert werden.

Um wieder ein Beispiel zu geben: Alle Rechner, die am gleichen Ethernetkabel angeschlossen sind, befinden sich in der Regel *im gleichen Subnetz* und sind direkt erreichbar. Auch wenn das Ethernet über Switches oder Bridges unterteilt ist, sind diese Rechner immer noch direkt erreichbar.

Wollen Sie eine längere Strecke überbrücken, ist das preiswerte Ethernet dafür nicht mehr geeignet. Sie müssen dann die IP-Pakete auf andere Hardware (z. B. FDDI oder ISDN) weiterleiten. Solche Geräte heißen Router bzw. Gateway. Ein Linuxrechner kann diese Aufgabe selbstverständlich auch erledigen, die entsprechende Option wird mit `ip_forwarding` bezeichnet.

Ist ein Gateway konfiguriert, wird das IP-Paket an das passende Gateway geschickt. Dieses versucht, das Paket dann wiederum nach dem gleichen Schema weiterzuleiten. Das wiederholt sich auf jedem weiteren Rechner sooft, bis das Paket entweder den Zielrechner erreicht hat oder die „Lebenszeit" TTL (engl. *time to live*) des Paketes verbraucht ist.

Adressart	**Beschreibung**
Die Netzwerkbasisadresse	Das ist die Netzmaske UND eine beliebige Adresse aus dem Netz, also das was in Tabelle 12.3 auf der vorherigen Seite unter `Ergebnis` abgebildet ist. Diese Adresse kann keinem Rechner zugewiesen werden.
Die Broadcastadresse	Sie heißt soviel wie: „Sprich alle Rechner in diesem Subnetz an". Um sie zu erzeugen wird die Netzmaske binär invertiert und mit der Netzwerkbasisadresse ODER verknüpft. Obiges Beispiel ergibt also 192.168.0.255. Natürlich kann auch diese Adresse keinem Rechner zugewiesen werden.
Der Localhost	Die Adresse `127.0.0.1` ist auf jedem Rechner fest dem so genannten „Loopbackdevice" zugewiesen. Über diese Adresse kann man eine Verbindung auf den eigenen Rechner aufbauen.

Tabelle 12.4: *Spezielle Adressen*

Da die IP-Adressen aber weltweit eindeutig sein müssen, können Sie natürlich nicht beliebige Adressen erfinden. Damit Sie aber trotzdem ein auf IP basierendes Netzwerk aufbauen können gibt es drei Adressbereiche, die Sie ohne weiteres verwenden können. Mit diesen können Sie allerdings nicht so ohne weiteres Verbindungen in das Internet aufbauen, da diese Adressen im Internet nicht weitergeleitet werden.

Dabei handelt es sich um diese Adressbereiche die in RFC 1597 definiert sind:

Netzwerk, Netzmaske	Bereich
10.0.0.0, 255.0.0.0	10.x.x.x
172.16.0.0, 255.240.0.0	172.16.x.x - 172.31.x.x
192.168.0.0, 255.255.0.0	192.168.x.x

Tabelle 12.5: *Private IP-Adressbereiche*

Domain Name System

DNS

DNS sorgt dafür, dass Sie sich nicht zwingend irgendwelche IP-Adressen merken müssen: Mit Hilfe von DNS kann eine IP-Adresse einem oder sogar mehreren Namen zugeordnet werden und umgekehrt auch eine Name einer IP-Adresse. Unter Linux erfolgt diese Umwandlung üblicherweise von einer speziellen Software namens bind. Der Rechner, der diese Umwandlung dann erledigt, nennt sich `Nameserver`. Dabei bilden die Namen wieder ein hierarchisches System, in dem die einzelnen Namensbestandteile durch Punkte getrennt sind. Die Namenshierarchie ist aber unabhängig von der oben beschriebenen Hierarchie der IP-Adressen.

Schauen wir uns einmal einen vollständigen Namen an, z. B. `laurent.suse.de` geschrieben im Format `Rechnername.Domain` . Ein vollständiger Name – Experten sagen „fully qualified domain name" oder kurz `FQDN` dazu – besteht aus einem Rechnernamen und einem Domainteil. Dabei wird der Domainteil aus einem frei wählbaren Anteil – im obigen Beispiel `suse` – und der so genannten `Top level domain`, `TLD` gebildet.

Aus historischen Gründen ist die Zuteilung der TLDs etwas verwirrend. So werden in den USA dreibuchstabige TLDs verwendet, woanders aber immer die aus zwei Buchstaben bestehenden ISO-Länderbezeichnungen.

In der Frühzeit des Internets (vor 1990) gab es hierzu eine Datei `/etc/hosts`, in der die Namen aller im Internet vertretenen Rechner gespeichert waren. Dies erwies sich bei der schnell wachsenden Menge von am Internet angeschlossener Rechner als unpraktikabel. Deshalb wurde eine dezentrale Datenbank entworfen, die die Rechnernamen verteilt speichern kann. Diese Datenbank, eben jener oben erwähnte Nameserver, hält also nicht die Daten aller Rechner im Internet vorrätig, sondern kann Anfragen an ihm nachgeschaltete, andere Nameserver weiterdelegieren.

An der Spitze der Hierarchie befinden sich die „Root-Nameserver", die die Top level domains verwalten. Die Root-Nameserver werden vom Network Information Center (NIC) verwaltet. Der Root-Nameserver kennt die jeweils für eine Top level domain zuständigen Nameserver. Im Falle der deutschen Top level domain de ist das DE-NIC für die Domains zuständig, die mit der TLD de aufhören. Mehr Informationen zum DE-NIC erhalten Sie auf der Website http://www.denic.de, mehr Informationen zum Top level domain NIC erfahren Sie unter http://www.internic.net.

Damit auch Ihr Rechner einen Namen in eine IP-Adresse auflösen kann, muss ihm mindestens ein Nameserver mit einer IP-Adresse bekannt sein. Die Konfiguration eines Nameservers erledigen Sie komfortabel mit Hilfe von YaST2 . Falls Sie eine Einwahl über Modem vornehmen, kann es sein, dass das zur Einwahl verwendete Protokoll die Adresse des Nameservers während der Einwahl mitliefert.

Aber nicht nur Rechnernamen können über DNS aufgelöst werden, DNS kann noch mehr. Zum Beispiel „weiß" der Nameserver auch, welcher Rechner für eine ganze Domain E-Mails annimmt, der so genannte Mail exchanger (MX).

Die Konfiguration des Nameserverzugriffs unter SuSE Linux ist im Abschnitt *DNS – Domain Name Service* auf Seite 297 beschrieben.

whois

Eng verwandt mit DNS ist das Protokoll whois. Mit dem gleichnamigen Programm whois können Sie schnell herauskriegen, wer für eine bestimmte Domain verantwortlich ist.

IPv6 – Internet der nächsten Generation

Warum ein neues Internet-Protokoll?

Bedingt durch die Erfindung des WWW (engl. *World Wide Web*) ist das Internet und damit die Anzahl der Rechner, die TCP/IP „sprechen", in den letzten zehn Jahren explosionsartig gewachsen. Seit der Erfindung des WWW durch Tim Berners-Lee 1990 am CERN (http://public.web.cern.ch/) ist die Zahl der Internet-Hosts von wenigen tausend auf mittlerweile ca. 100 Millionen gewachsen.

Wie Sie wissen, besteht eine IP-Adresse „nur" aus 32 Bit. Viele IP-Adressen können durch organisatorische Bedingtheiten gar nicht verwendet werden,

sie gehen verloren. Zur Erinnerung: Das Internet wird in Subnetze, also Teilnetze unterteilt. Diese bestehen immer aus einer Zweierpotenz minus zwei nutzbaren IP-Adressen. Ein Subnetz besteht also beispielsweise aus 2, 6, 14, 30 usw. IP-Adressen. Möchten Sie beispielsweise 128 Rechner an das Internet anbinden, so benötigen Sie ein „Class C" Subnetz mit 256 IP-Adressen, von denen nur 254 nutzbar sind. Wie Sie oben gesehen haben, entfallen zwei der IP-Adressen aus einem Subnetz, nämlich die Broadcastadresse und die Netzwerkbasisadresse.

Die Konfiguration eines Rechners im TCP/IP-Netzwerk ist relativ kompliziert. Wie Sie oben schon gesehen haben, müssen Sie auf Ihrem Rechner folgende Dinge konfigurieren: Die eigene IP-Adresse, Subnetzmaske, Gatewayadresse (falls vorhanden) und einen Nameserver. Diese Daten müssen Sie alle „wissen" bzw. von Ihrem Provider bekommen, sie können nicht irgendwoher abgeleitet werden. In jedem IP-Paket ist eine Prüfsumme enthalten, die bei jedem Routingvorgang überprüft und neu berechnet werden muss. Deshalb benötigen sehr schnelle Router leider sehr viel Rechenleistung, was diese Router verteuert.

Einige Dienste werden bisher mit Broadcasts realisiert (zum Beispiel das Windows Netzwerkprotokoll SMB). Rechner, die nicht an diesem Dienst interessiert sind, sind trotzdem gezwungen, die Pakete zu verarbeiten um sie dann anschließend zu ignorieren. In sehr schnellen Netzwerken kann das durchaus ein Problem werden.

Der Nachfolger des bisherigen IP, IPv6, löst all diese Probleme. Das primäre Ziel bei der Entwicklung war, den beschränkten Adressraum stark zu erweitern und die Konfiguration von Arbeitsstationen zu vereinfachen, wenn möglich zu automatisieren. In diesem Abschnitt wird von IPv4 oder IP die Rede sein, wenn das bisher verwendete und verbreitete Internet-Protokoll gemeint ist, und von IPv6, wenn es um die neue Version 6 geht.

IPv6 ist in RFC 1752 näher erläutert. IPv6 verwendet 128-Bit-Adressen, bietet also viele Billiarden IP-Adressen, genug auch bei großzügiger Verteilung der Adressen. Diese enorme Menge an IPv6-Adressen erlaubt den Luxus, das kleinste Subnetz 48 Bit „groß" zu machen.

Dies erlaubt dann nämlich auch, die oben erläuterte MAC-Adresse als Adressbestandteil zu verwenden. Da diese weltweit nur einmal vorhanden und zugleich vom Hardwarehersteller fest vorgegeben ist, vereinfacht sich die Konfiguration der Rechner sehr. In Wirklichkeit werden sogar die ersten 64 Bit zu einem so genannten `EUI-64`-Token zusammengefasst. Dabei werden die letzten 48 Bit der MAC-Adresse entnommen, die restlichen 24 Bit enthalten spezielle Informationen, die etwas über den Typ des Tokens aussagen. Das ermöglicht dann auch, Geräten ohne MAC-Adresse (PPP- und ISDN-Verbindungen!) ein `EUI-64`-Token zuzuweisen.

Zusätzlich gibt es in IPv6 eine neue Erfindung: Einer Netzwerkschnittstelle werden üblicherweise mehrere IP-Adressen zugewiesen. Das hat den Vorteil, dass mehrere verschiedene Netze zur Verfügung stehen. Eines davon kann mit Hilfe der MAC-Adresse und einem bekannten Präfix zu einem vollautomatisch konfigurierten Netz zusammengestellt werden, und ohne weitere Konfigurationsarbeiten sind damit direkt nach dem Starten von IPv6 alle Rechner im lokalen Netz erreichbar (sog. „Link-local-Adresse“).

Aber auch die restliche Konfiguration einer Arbeitsstation kann weitgehend automatisch erfolgen. Hierzu gibt es ein spezielles Protokoll, mit dem Arbeitsstationen von einem Router eine IP-Adresse bekommen können.

Zwingend vorgeschrieben für alle IPv6 unterstützenden Rechner ist die Unterstützung von „Multicast“. Mit Hilfe von Multicast kann eine Gruppe von Rechnern auf einmal angesprochen werden, also nicht alle auf einmal („broadcast“), oder nur einer („unicast“), sondern eben ein paar. Welche das sind, hängt von der Anwendung ab. Es gibt aber auch ein paar wohldefinierte Multicastgruppen, beispielsweise „alle Nameserver“ (engl. *all nameservers multicast group*), oder „alle Router“ (engl. *all routers multicast group*).

Da eine plötzliche Umstellung aller Rechner im Internet von IPv4 auf IPv6 nicht denkbar ist, gibt es einen Kompatibilitätsmodus. Dieser bildet die bisherigen Adressen auf IPv6-Adressen ab. Gleichzeitig gibt es Mechanismen wie „Tunneling“. Hierbei werden IPv6-Pakete in IPv4-Paketen verpackt verschickt. Natürlich sind auch Umsetzungen von IPv6 auf IPv4 und umgekehrt möglich. Um einen IPv6-Rechner von einem IPv4-Rechner aus erreichen zu können, ist es allerdings nötig, dass der IPv6-Rechner eine IPv4-Kompatibilitätsadresse hat.

Aufbau einer IPv6-Adresse

Sie können sich sicher vorstellen, dass eine IPv6-Adresse, bedingt durch die 128 Bit, wesentlich länger wird als eine IPv4-Adresse mit Ihren 32 Bit. Immerhin ist eine IPv6-Adresse damit 16 Byte lang. Verursacht durch die Größe werden die neuen IPv6-Adressen in einer anderen Schreibweise geschrieben als die bisher verwendeten IPv4-Adressen. Schauen wir uns einmal die Beispiele in Tabelle 12.6 auf der nächsten Seite an.

Wie Sie der Tabelle entnehmen, werden IPv6-Adressen mit Hilfe von Hexadezimalzahlen dargestellt. Die Hexadezimalzahlen werden immer zu je zwei Byte gruppiert zusammengefasst und durch `:` getrennt dargestellt. Es gibt daher maximal acht Gruppen und sieben Doppelpunkte in einer Adresse. Führende Null-Bytes in einer Gruppe dürfen weggelassen werden, nicht aber inmitten oder am Ende einer Gruppe. Mehr als vier Null-Bytes direkt hintereinander kann man durch das Auslassungszeichen `::` überspringen. Allerdings

Bezeichnung	Adresswert
Localhost	`::1`
IPv4 kompatible IPv6-Adresse	`::10.10.11.102` (IPv6 wird unterstützt)
IPv4 gemappte IPv6-Adresse	`::ffff:10.10.11.102` (IPv6 wird nicht unterstützt)
beliebige Adresse	`3ffe:400:10:100:200:c0ff:fed0:a4c3`
Link-local-Adresse	`fe80::10:1000:1a4`
Site-local-Adresse	`fec0:1:1:0:210:10ff:fe00:1a4`
Multicastgruppe „alle link-lokalen Router“	`ff02:0:0:0:0:0:0:2`

Tabelle 12.6: *Darstellung verschiedener IPv6 Adressen*

ist nur ein Auslassungszeichen in einer Adresse erlaubt. Dieser Vorgang des Auslassens wird in Englisch mit „collapsing“ bezeichnet. Eine Spezialdarstellung sind IPv4-Kompatibilitätsadressen: Hier wird die IPv4-Adresse einfach an den festgelegten Präfix für IPv4-Kompatibilitätsadressen angehängt.

Jeder Teil einer IPv6-Adresse hat eine definierte Bedeutung. Die ersten Bytes bilden einen Präfix und geben den Typ der Adresse an. Der Mittelteil adressiert ein Netzwerk oder ist bedeutungslos und den Schluss der Adresse bildet der Hostteil.

Tabelle 12.7 auf der nächsten Seite veranschaulicht die Bedeutung einiger häufiger Präfixe.

Präfix(hexadez.)	Verwendung
`00`	IPv4 und IPv4 über IPv6-Kompatibilitätsadressen. Es handelt sich um eine zu IPv4 kompatible Adresse. Ein geeigneter Router muss das IPv6-Paket noch in IPv4 verwandeln. Weitere Spezialadressen (z. B. Loopback Device) sind ebenfalls mit diesem Präfix ausgestattet.
erste Ziffer 2 oder 3	(engl. *provider-based-unicast*) Provider basierte Unicast-Adressen. Wie bisher auch können Sie bei IPv6 von einem Provider Teilnetze zugewiesen bekommen.
`fe80` bis `febf`	(engl. *link-local*) Adressen mit diesem Präfix dürfen nicht geroutet werden und können daher nur im gleichen Subnetz erreicht werden.
`fec0` bis `feff`	(engl. *site-local*) Diese Adressen dürfen zwar geroutet werden, aber nur innerhalb einer Organisation. Damit entsprechen diese Adressen den bisherigen „privaten" Netzen (beispielsweise `10.x.x.x`).
`ff`	(engl. *multicast*) IPv6-Adressen die mit `ff` anfangen sind Multicastadressen.

Tabelle 12.7: *verschiedene IPv6-Präfixe*

Wie Sie oben schon sehen, sind speziell Unicastadressen sehr lang. Diese kann man sich praktisch nicht mehr merken. Ein funktionierender Nameserver ist für IPv6 daher noch wichtiger als bei IPv4. Der Nameserver ist so wichtig, dass es ein spezielles Autokonfigurationsprotokoll für Nameserver gibt.

IPv6-Netzmasken

Netzmasken werden in IPv6 etwas anders dargestellt. Da schon von Anfang an klassenloses Routing verwendet wird und schon das kleine Subnetz praktisch beliebig viele Rechner aufnehmen kann, macht die Unterteilung der Netze in Klassen keinen Sinn. Da die Netzmasken in der Darstellung sehr lang wären, werden diese nun ganz anders geschrieben. Die Schreibweise

```
fec0:1:1:0:210:10ff:fe00:1a4/64
```

bedeutet, dass die letzten 64 Bit den Hostteil und die vorderen 64 Bit den Netzwerkteil der Adresse bilden.

Anders gesagt bedeutet die 64, dass von links her die Netzmaske mit 1 Bits aufgefüllt wird. Es gibt in der Netzmaske also 64 1 Bits. Wie bei IPv4 wird durch eine UND-Verknüpfung der Netzmaske mit der IP-Adresse bestimmt, ob sich ein Rechner im gleichen oder in einem anderen Subnetz befindet.

Weiterführende Literatur und Links zu IPv6

Natürlich kann und will der obige Überblick keine vollständige Einführung zum sehr umfangreichen Thema IPv6 sein. Zum tieferen Einstieg in IPv6 können Sie die folgende Onlineliteratur und Bücher zu Rate ziehen:

http://www.bieringer.de/linux/IPv6/ Linux-IPv6-HOWTO und viele Links.

http://www.6bone.de/ Anschluss an das IPv6 über einen Tunnel bekommen.

http://www.ipv6.org/ Alles rund um IPv6.

RFC 1725 Das einführende RFC zum Thema IPv6.

Die Einbindung ins Netzwerk

TCP/IP ist inzwischen das Standard-Netzwerkprotokoll, über das alle modernen Betriebssysteme mit TCP/IP kommunizieren können. Dennoch unterstützt Linux auch noch andere Netzwerkprotokolle, beispielsweise das (früher) von Novell Netware verwendete IPX oder das von Macintosh-Rechnern verwendete Appletalk. In diesem Rahmen besprechen wir nur die Integration eines Linux-Rechners in ein TCP/IP-Netzwerk. Wenn Sie „exotische“ Arcnet, Token-Ring oder FDDI-Netzwerkkarten einbinden wollen, finden Sie weiterführende Hilfe hierzu in den Kernelquellen `/usr/src/linux/Documentation`. Änderungen in der Netzwerk-Konfiguration seit SuSE Linux 8.0 sind in folgender Datei dokumentiert: `/usr/share/doc/packages/sysconfig/README`.

Vorbereitungen

Der Rechner muss über eine unterstützte Netzwerkkarte verfügen. Üblicherweise wird die Netzwerkkarte schon bei der Installation erkannt und der passende Treiber eingebunden. Ob Ihre Karte korrekt eingebunden wurde, können Sie unter anderem daran sehen, dass die Ausgabe des Kommandos `ifstatus eth0` das Netzwerk-Device `eth0` anzeigt.

Wenn der Kernel-Support für die Netzwerkkarte als Modul realisiert wird – so wie es beim SuSE-Kernel standardmäßig der Fall ist –, dann muss der Name des Moduls als Alias in der `/etc/modules.conf` eingetragen werden. Für die erste Ethernet-Karte z. B. in dieser Art: `alias eth0 tulip`. Dies geschieht automatisch, wenn im linuxrc während der Erstinstallation der Treiber-Support für die Netzwerkkarte geladen wird. Nachträglich lässt sich diese Aufgabe von YaST2 aus erledigen.

Bei hotplugfähigen Netzwerkkarten (z. B. PCMCIA oder USB) werden die Treiber beim Einstecken automatisch ermittelt; es muss dazu nichts konfiguriert werden. Details dazu finden Sie in Kapitel *Hotplug* auf Seite 143.

Konfiguration mit YaST2

Die Konfiguration der Netzwerkkarte lässt sich mit YaST2 schnell durchführen. Wählen Sie im Kontrollzentrum den Punkt ‘Netzwerk/Basis’ und anschließend ‘Konfiguration der Netzwerkkarte’. In diesem Dialog integrieren Sie mit ‘Hinzufügen’ eine Netzwerkkarte, mit ‘Entfernen’ wird die entsprechende Karte aus der Konfiguration gelöscht und mit ‘Bearbeiten’ können die Einstellungen zu einer Netzwerkkarte geändert werden.

Aktivieren Sie den Punkt 'Hardware', um die Hardwaredaten einer schon eingerichteten Netzwerkkarte mit 'Bearbeiten' zu verändern. Sie gelangen in das Menü zur Konfiguration der Hardwaredaten Ihrer Netzwerkkarte; vgl. Abbildung 12.3.

Üblicherweise wird der richtige Treiber für Ihre Netzwerkkarte schon während der Installation von YaST2 konfiguriert und die Netzwerkkarte aktiviert. Daher sind manuelle Einstellungen der Hardwareparameter nur nötig, wenn Sie mehr als eine Netzwerkkarte einsetzen oder die Netzwerkhardware nicht automatisch erkannt wird. In diesem Fall müssen Sie den Punkt 'Hinzufügen' anwählen, damit ein neues Treibermodul ausgewählt werden kann.



Abbildung 12.3: *Konfiguration der Hardwareparameter*

In diesem Dialog können Sie den Typ der Netzwerkkarte und im Falle von ISA-Karten auch den zu verwendenden Interrupt und die IO-Adresse einstellen. Manchen Netzwerktreibern können Sie auch spezielle Parameter wie die zu verwendende Schnittstelle mitgeben, ob Sie beispielsweise den `RJ-45`- oder `BNC`-Anschluss auf der Karte verwenden wollen. Beachten Sie hierzu die Dokumentation des Treibermoduls. Für PCMCIA und USB genügt es die entsprechenden Kästchen zu aktivieren.

Nach der Eingabe der Hardwareparameter konfigurieren Sie die weiteren Daten der Netzwerkschnittstelle. Wählen Sie im Dialog 'Grundlegende Netzwerkkonfiguration' den Punkt 'Schnittstelle' aus, um die soeben einrichtete Netzwerkkarte zu aktivieren und dieser Netzwerkkarte eine IP-Adresse zuzuweisen. Wählen Sie dann die Kartennummer aus und klicken Sie auf 'Be-

arbeiten'. Es erscheint ein neuer Dialog, in dem Sie die IP-Adresse und die weiteren Daten des IP-Netzwerks auswählen können. Falls Sie selbst ein eigenes Netzwerk aufbauen, können Sie sich bei der Vergabe der Adressen am Abschnitt 12 auf Seite 270 bzw. der Tabelle 12.5 auf Seite 277 orientieren. Ansonsten tragen Sie bitte die von Ihrem Netzwerkadministrator zugewiesenen Adressen in die vorgesehenen Felder ein.

Vergessen Sie nicht, einen Nameserver unter 'Rechnername und Nameserver' einzustellen, damit die Namensauflösung wie in Abschnitt 12 auf Seite 297 beschrieben funktionieren kann. Über den Punkt 'Routing' können Sie das Routing einstellen. Wählen Sie den Punkt 'Konfiguration für Experten', um fortgeschrittene Einstellungen vorzunehmen.

Falls Sie Funknetzwerkkarten verwenden, aktivieren Sie bitte das Kästchen 'Wireless Device'. Sie können dann die wichtigsten Einstellungen hierzu in einem eigenen Dialog vornehmen. Im Wesentlichen sind das der Betriebsmodus, Netzwerknamen und ein Schlüssel für die verschlüsselte Datenübertragung.

Damit ist die Netzwerkkonfiguration abgeschlossen. YaST2 ruft abschließend SuSEconfig auf und trägt Ihre Angaben in die entsprechenden Dateien ein. Damit die Einstellungen wirksam werden, müssen die betroffenen Programme neu konfiguriert und die entsprechenden Daemonen neu gestartet werden. Dies erreichen Sie, indem Sie folgenden Befehl eingeben:

```
erde:~ #  rcnetwork restart
```

Hotplug/PCMCIA

Eine Sonderstellung nehmen hotplugfähige Netzwerkkarten ein wie z. B. PCMCIA oder USB-Geräte. Im Gegensatz zu fest eingebauten Netzwerkkarten, die eine gleich bleibende Gerätebezeichnung erhalten, beispielsweise `eth0`, wird solchen Karten dynamisch bei Bedarf eine freie Gerätebezeichnung zugewiesen. Um Konflikte mit eventuell fest eingebauten Karten zu vermeiden wird PCMCIA und Hotplug beim Booten auch erst nach dem Netzwerk gestartet.

Diese Karten werden automatisch eingerichtet sobald sie eingesetzt bzw. beim Booten erkannt werden. Deshalb ist es nicht notwendig, dass PCMCIA vor dem Netzwerk gestartet wird. Im Gegenteil: Wenn diese Karten nur vom Netzwerkstartscript beim Booten behandelt würden, ginge die Möglichkeit, sie zur Laufzeit des Systems zu tauschen, verloren.

Konfiguration von IPv6

Falls Sie die Verwendung von IPv6 konfigurieren möchten, müssen Sie in der Regel keine Konfiguration auf den Arbeitsstationen durchführen. Allerdings muss die IPv6-Unterstützung geladen werden. Dies können Sie am einfachsten mit dem Kommando

```
erde:~ #  modprobe ipv6
```

erledigen. Aufgrund der Autokonfigurationsphilosophie von IPv6 wird dann der Netzwerkkarte eine Adresse im `link-local` Netz zugewiesen. Normalerweise wird auf einer Arbeitsstation keine Routingtabelle gepflegt. Die Router im Netz können über das `Router Advertisment Protocol` von der Arbeitsstation darüber befragt werden, welches Präfix und welche Gateways zu verwenden sind. Um einen IPv6-Router aufzusetzen, können Sie das Programm radvd aus Paket `radvd` verwenden. Dieses Programm teilt den Arbeitsstationen das zu verwendende Präfix für IPv6-Adressen und den/die Router mit.

Um einer Arbeitsstation eine IPv6-Adresse bequem zuweisen zu können, ist es also ratsam, einen Router mit dem Programm radvd zu installieren und zu konfigurieren. Die Arbeitsstationen bekommen die IPv6-Adresse dann automatisch zugewiesen.

Manuelle Netzwerkkonfiguration

Die manuelle Konfiguration der Netzwerksoftware sollte stets die zweite Wahl sein. Wir empfehlen, YaST2 zu benutzen.

Wesentlich ist hier, dass alle Netzwerk-Interfaces mit dem Script `/sbin/ifup` aufgesetzt werden. Zum Anhalten oder Prüfen eines Interfaces gibt es `ifdown` und `ifstatus`.

Wenn Sie haben nur festeingebaute Netzwerkkarten haben, genügt es die Interfaces über ihren Namen zu konfigurieren. Mit `ifup eth0`, `ifstatus eth0` und `ifdown eth0` starten, prüfen und stoppen Sie das Netzwerkinterface `eth0`. Die verwendeten Konfigurationsdaten liegen unter `/etc/sysconfig/network/ifcfg-eth0`. `eth0` ist hier sowohl der Interface-Name als auch der Name für die Netzwerkkonfiguration.

Die Netzwerkkonfiguration kann alternativ auch der Hardware-Adresse (MAC-Adresse) einer Netzwerkkarte zugeordnet werden. Dazu wird eine Konfigurationsdatei `ifcfg-<HardwareadresseohneDoppelpunkte>`

verwendet. Die Buchstaben der Hardware-Adresse müssen hier klein geschrieben werden, so wie sie von `ip link` ausgegeben wird (`ifconfig` verwendet große Buchstaben). Wenn `ifup` eine Konfigurationsdatei passend zur Hardware-Adresse findet, wird ein möglicherweise auch vorhandenes `ifcfg-eth0` ignoriert.

Mit hotplugfähigen Netzwerkkarten wird es ein wenig komplizierter. Wenn Sie keine solche Karte besitzen, können Sie beim Abschnitt *Konfigurationsdateien* auf der nächsten Seite weiterlesen.

Da bei hotplugfähigen Netzwerkkarten die Zuordnung des Interface-Namen zur Karte eher zufällig ist, werden die Konfigurationen für eine solche Karte nicht unter dem Interface-Namen abgelegt, sondern unter einem Bezeichner, der die Art der verwendeten Hardware und den Anschlusspunkt beschreibt, im Folgenden Hardwarebeschreibung genannt. `ifup` muss in diesem Fall mit zwei Argumenten aufgerufen werden, der genauen Hardwarebeschreibung und dem gegenwärtigen Interface-Namen. Anschließend wird von `ifup` die Konfiguration ermittelt, die möglichst genau auf die Hardwarebeschreibung passt.

Als Beispiel wollen wir einen Laptop mit zwei PCMCIA-Steckplätzen und einer PCMCIA Ethernet Netzwerkkarte annehmen. Außerdem gibt es in diesem Gerät noch eine festeingebaute Netzwerkkarte, die als Interfacenamen `eth0` erhält. Wenn diese Karte im Steckplatz `0` steckt, lautet ihre Hardwarebeschreibung `eth-pcmcia-0`. Der cardmgr oder das Hotplug-Netzwerkscript rufen nun `ifup eth-pcmcia-0 eth1` auf. Nun sucht `ifup`, ob es unter `/etc/sysconfig/network/` eine Datei `ifcfg-eth-pcmcia-0` gibt. Wenn nicht wird weiter nach `ifcfg-eth-pcmcia`, `ifcfg-pcmcia-0`, `ifcfg-pcmcia`, `ifcfg-eth1` und `ifcfg-eth` gesucht. Die zuerst gefundene Datei wird zur Konfiguration verwendet. Wenn also eine Netzwerkkonfiguration angelegt werden soll, die für alle PCMCIA-Netzwerkkarten (in allen Steckplätzen) gelten soll, muss diese `ifcfg-pcmcia` heißen. Diese würde dann für `eth-pcmcia-0` genauso wie für eine Tokenringkarte in Steckplatz 1 `tr-pcmcia-1` verwendet.

Auch hier hat wieder eine Konfiguration nach Hardwareadresse absoluten Vorrang. Dies wurde nur aus Gründen der Übersichtlichkeit aus dem Beispiel weggelassen.

YaST2 geht bei der Konfiguration von hotplugfähigen Karten einen Umweg. Dort werden Konfigurationen für solche Karten durchnummeriert. Deshalb schreibt YaST2 die Einstellungen für eine PCMCIA-Karte immer nach `ifcfg-eth-pcmcia-<laufendeNummer>`. Damit diese Konfiguration dann trotzdem für alle Steckplätze funktioniert, wird noch ein Link `ifcfg-eth-pcmcia` auf diese Datei angelegt. Dies sollten Sie beachten, wenn Sie teilweise mit und teilweise ohne YaST2 konfigurieren.

Konfigurationsdateien

Dieser Abschnitt gibt eine Übersicht über die Netzwerkkonfigurationsdateien und erklärt ihre Funktion sowie das verwendete Format.

`/etc/sysconfig/network/ifcfg-*` Diese Dateien enthalten die Daten, die spezifisch für ein Netzwerk-Interface sind. Sie können nach dem Interface-Namen benannt sein (`ifcfg-eth2`), nach der Hardware-Adresse einer Netzwerkkarte (`ifcfg-000086386be3`) oder nach einer Hardware-Beschreibung für eine Karte (`ifcfg-usb`). Sollen Netzwerkaliase verwendet werden, heißen die dazu nötigen Dateien einfach `ifcfg-eth2:1` oder `ifcfg-usb:1`. Das Script `ifup` bekommt neben dem Interface-Namen bei Bedarf auch eine genaue Hardwarebeschreibung und sucht dann die am besten passende Datei zur Konfiguration aus.

Die Dateien enthalten die IP-Adresse (BOOTPROTO="static", IPADDR="10.10.11.214") oder die Anweisung, DHCP zu verwenden (BOOTPROTO="dhcp"). Die IP-Adresse kann die Netzmaske bereits enthalten (IPADDR="10.10.11.214/16") oder man kann diese extra angeben (NETMASK="255.255.0.0"). Die vollständige Liste von Variablen enthält Manual-Page von `ifup` (`man ifup`). Es können außerdem alle Variablen aus den Dateien `dhcp`, `wireless` und `config` in den `ifcfg-*`-Dateien verwendet werden, wenn eine sonst allgemeine Einstellung nur für ein Interface verwendet werden soll. Mit den Variablen `POST_UP_SCRIPT` und `PRE_DOWN_SCRIPT` können individuelle Scripte nach dem Starten oder vor dem Anhalten des Interfaces ausgeführt werden.

`/etc/sysconfig/network/config,dhcp,wireless` Die Datei `config` enthält allgemeine Einstellungen zum Verhalten von `ifup`, `ifdown` und `ifstatus`. Sie ist vollständig kommentiert. Ebenso gibt es Kommentare in `dhcp` und `wireless`, wo allgemeine Einstellungen zu DHCP und Funknetzwerkkarten Platz finden. Alle Variablen aus diesen Dateien können auch in `ifcfg-*` verwendet werden und haben dort natürlich vorrang.

`/etc/resolv.conf`
Wie bereits die Datei `/etc/host.conf`, so spielt auch diese Datei in Bezug auf Auflösung von Rechnernamen durch die *resolver*-Bibliothek eine Rolle.

In dieser Datei wird angegeben, welcher Domain der Rechner angehört (Schlüsselwort `search`) und wie die Adresse des Nameservers ist

(Schlüsselwort `nameserver`), der angesprochen werden soll. Es können mehrere Domainnamen angegeben werden. Beim Auflösen eines nicht voll qualifizierten Namens wird versucht, durch Anhängen der einzelnen Einträge in `search` einen gültigen, voll qualifizierten Namen zu erzeugen. Mehrere Nameserver können durch mehrere Zeilen, die mit `nameserver` beginnen, bekannt gemacht werden. Kommentare werden wieder mit '#' eingeleitet.

Ein Beispiel für `/etc/resolv.conf` zeigt Datei 16.

```
# Our domain
search kosmos.all
#
# We use sonne (192.168.0.1) as nameserver
nameserver 192.168.0.1
```

Datei 16: */etc/resolv.conf*

YaST trägt hier den angegebenen Nameserver ein!

Einige Dienste wie pppd (wvdial), ipppd (isdn), dhcp (dhcpcd und dhclient), pcmcia und hotplug modifizieren die Datei `/etc/resolv.conf` über das Skript `modify_resolvconf`.

Wenn die Datei `/etc/resolv.conf` durch dieses Skript vorübergehend modifiziert wurde, enthält sie einen definierten Kommentar, der Auskunft darüber gibt, welcher Dienst sie modifiziert hat, wo die ursprüngliche Datei gesichert ist und wie man die automatischen Modifikationen abstellen kann.

Wenn `/etc/resolv.conf` mehrmals modifiziert wird, wird diese Verschachtelung von Modifikationen auch dann wieder sauber abgebaut, wenn sie in einer anderen Reihenfolge zurückgenommen werden; dies kann bei isdn, pcmcia und hotplug durchaus vorkommen.

Wenn ein Dienst nicht sauber beendet wurde, kann mit Hilfe des Skripts `modify_resolvconf` der Ursprungszustand wiederhergestellt werden. Beim Booten wird geprüft, ob eine modifizierte `resolv.conf` stehen geblieben ist (z. B. wegen Systemabsturz). Dann wird die ursprüngliche (unmodifizierte) `resolv.conf` wiederhergestellt.

YaST findet mittels `modify_resolvconf check` heraus, ob `resolv.conf` modifiziert wurde, und dann den Benutzer warnen, dass seine Änderungen nach der Restauration wieder verloren sein werden. Ansonsten verwendet YaST `modify_resolvconf` nicht, das heißt eine Änderung der Datei resolv.conf mittels YaST und eine manuelle Änderung sind äquivalent. Beides entspricht einer gezielten und dauerhaften

Änderung, während eine Änderung durch einen der genannten Dienste nur vorübergehend ist.

/etc/hosts

In dieser Datei (siehe Datei 17) werden Rechnernamen IP-Adressen zugeordnet. Wird kein Nameserver verwendet, müssen hier alle Rechner aufgeführt werden, zu denen eine IP-Verbindung aufgebaut werden soll. Je Rechner wird eine Zeile bestehend aus IP-Adresse, dem voll qualifizierten Hostnamen und dem Rechnernamen (z. B. `erde`) in die Datei eingetragen. Die IP-Adresse muss am Anfang der Zeile stehen, die Einträge werden durch Leerzeichen bzw. Tabulatoren getrennt. Kommentare werden durch `'#'` eingeleitet.

```
127.0.0.1 localhost
192.168.0.1 sonne.kosmos.all sonne
192.168.0.20 erde.kosmos.all erde
```

Datei 17: */etc/hosts*

/etc/networks

Hier werden Netzwerknamen in Netzwerkadressen umgesetzt. Das Format ähnelt dem der `hosts`-Datei, jedoch stehen hier die Netzwerknamen vor den Adressen (siehe Datei 18).

```
loopback      127.0.0.0
localnet      192.168.0.0
```

Datei 18: */etc/networks*

/etc/host.conf

Das Auflösen von Namen – d. h. das Übersetzen von Rechner- bzw. Netzwerknamen über die *resolver*-Bibliothek – wird durch diese Datei gesteuert. Diese Datei wird nur für Programme verwendet, die gegen die libc4 oder die libc5 gelinkt sind; für aktuelle glibc-Programme vgl. die Einstellungen in `/etc/nsswitch.conf`! Ein Parameter muss in einer eigenen Zeile stehen, Kommentare werden durch `'#'` eingeleitet. Die möglichen Parameter zeigt Tabelle 12.8 auf der nächsten Seite.

order *hosts, bind*	Legt fest, in welcher Reihenfolge die Dienste zum Auflösen eines Namens angesprochen werden sollen. Mögliche Argumente sind (durch Leerzeichen oder Kommata voneinander getrennt): *hosts*: Durchsuchen der Datei `/etc/hosts` *bind*: Ansprechen eines Nameservers *nis*: Über NIS
multi *on/off*	Bestimmt, ob ein in `/etc/hosts` eingetragener Rechner mehrere IP-Adressen haben darf.
nospoof *on* alert *on/off*	Diese Parameter beeinflussen das *spoofing* des Nameservers, haben aber weiter keinen Einfluss auf die Netzwerkkonfiguration.
trim ⟨*domainname*⟩	Der angegebene Domainname wird vor dem Auflösen des Rechnernamens von diesem abgeschnitten (insofern der Rechnername diesen Domainnamen enthält). Diese Option ist dann von Nutzen, wenn in der Datei `/etc/hosts` nur Namen aus der lokalen Domain stehen, diese aber auch mit angehängtem Domainnamen erkannt werden sollen.

Tabelle 12.8: *Parameter für /etc/host.conf*

Ein Beispiel für `/etc/host.conf` zeigt Datei 19.

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

Datei 19: *`/etc/host.conf`*

`/etc/nsswitch.conf`

Mit der GNU C Library 2.0 hat der „Name Service Switch“ (NSS) Einzug gehalten (vgl. Manual-Page von `nsswitch.conf` (`man 5 nsswitch.conf`), sowie ausführlicher *The GNU C Library Reference Manual*, Kap. "System Databases and Name Service Switch"; vgl. Paket `libcinfo`).

In der Datei `/etc/nsswitch.conf` wird festgelegt, in welcher Reihenfolge bestimmte Informationen abgefragt werden. Ein Beispiel für `nsswitch.conf` zeigt Datei 20. Kommentare werden durch '#' eingeleitet. Dort bedeutet z. B. der Eintrag bei der „Datenbank" `hosts`, dass nach `/etc/hosts` (`files`) eine Anfrage über DNS (vgl. Abschnitt 12 auf Seite 297) losgeschickt wird.

```
passwd:     compat
group:      compat

hosts:      files dns
networks:   files dns

services:   db files
protocols:  db files

netgroup:   files
automount:  files nis
```

***Datei 20:** `/etc/nsswitch.conf`*

Die über NSS verfügbaren „Datenbanken" sind in Tabelle 12.9 auf der nächsten Seite genannt. Zusätzlich sind in Zukunft `automount`, `bootparams`, `netmasks` und `publickey` zu erwarten.

`aliases`	Mail-Aliase, von `sendmail`(8) verwendet; vgl. Manual-Page von `aliases` (`man 5 aliases`).
`ethers`	Ethernet-Adressen.
`group`	Für Benutzergruppen, von `getgrent`(3) verwendet; vgl. Manual-Page von `group` (`man 5 group`).
`hosts`	Für Hostnamen und IP-Adressen, von `gethostbyname`(3) und ähnlichen Funktionen verwendet.
`netgroup`	Im Netzwerk gültige Liste von Hosts und Benutzern, um Zugriffsrechte zu steuern; vgl. Manual-Page von `netgroup` (`man 5 netgroup`).
`networks`	Netzwerknamen und -adressen, von `getnetent`(3) verwendet.
`passwd`	Benutzerpasswörter, von `getpwent`(3) verwendet; vgl. Manual-Page von `passwd` (`man 5 passwd`).

***Tabelle 12.9:** Fortsetzung auf der nächsten Seite. . .*

`protocols`	Netzwerk-Protokolle, von `getprotoent`(3) verwendet; vgl. Manual-Page von `protocols` (`man 5 protocols`).
`rpc`	„Remote Procedure Call"-Namen und -Adressen, von `getrpcbyname`(3) und ähnlichen Funktionen verwendet.
`services`	Netzwerkdienste, von `getservent`(3) verwendet.
`shadow`	„Shadow"-Passwörter der Benutzer, von `getspnam`(3) verwendet; vgl. Manual-Page von `shadow` (`man 5 shadow`).

Tabelle 12.9: *Über /etc/nsswitch.conf verfügbare Datenbanken*

Die Konfigurationsmöglichkeiten der NSS-„Datenbanken" stehen in Tabelle 12.10.

`files`	direkt auf Dateien zugreifen, z. B. auf `/etc/aliases`.
`db`	über eine Datenbank zugreifen.
`nis`	NIS, vgl. Abschnitt 12 auf Seite 307.
`nisplus`	
`dns`	Nur bei `hosts` und `networks` als Erweiterung verwendbar.
`compat`	Nur bei `passwd`, `shadow` und `group` als Erweiterung verwendbar.
zusätzlich	ist es möglich, unterschiedliche Reaktionen bei bestimmten Lookup-Ergebnissen auszulösen; Details sind der Manual-Page von `nsswitch.conf` (`man 5 nsswitch.conf`) zu entnehmen.

Tabelle 12.10: *Konfigurationsmöglichkeiten der NSS-„Datenbanken"*

`/etc/nscd.conf`

Über diese Datei wird der nscd (engl. *Name Service Cache Daemon*) konfiguriert (vgl. Manual-Page von `nscd` (`man 8 nscd`) und Manual-Page von `nscd.conf` (`man 5 nscd.conf`)). Betroffen sind die Informationen von `passwd` und `groups`. `hosts` wird nicht eingelesen, damit der Daemon nicht neu gestartet werden muss, wenn z. B. die Namensauflö-

sung (DNS) durch Änderung der /etc/resolv.conf umgestellt wird.

Wenn beispielsweise das Caching für passwd aktiviert ist, dauert es in der Regel 15 Sekunden, bis ein neu angelegter lokaler Benutzer dem System bekannt ist. Durch das Neustarten des nscd kann diese Wartezeit verkürzt werden:

```
erde:~ #  rcnscd restart
```

/etc/HOSTNAME
Hier steht der Name des Rechners, also nur der Hostname ohne den Domainnamen. Diese Datei wird von verschiedenen Skripten während des Starts des Rechners gelesen. Sie darf nur eine Zeile enthalten, in der der Rechnername steht!

Startup-Skripten

Neben den beschriebenen Konfigurationsdateien gibt es noch verschiedene Skripten, die während des Hochfahrens des Rechners die Netzwerkprogramme starten. Diese werden gestartet, sobald das System in einen der *Multiuser-Runlevel* übergeht (vgl. Tabelle 12.11).

/etc/init.d/network	Dieses Skript übernimmt die Konfiguration der Netzwerk Hard- und Software während der Startphase des Systems.
/etc/init.d/inetd	Startet den inetd. Dies ist beispielsweise dann nötig, wenn Sie sich vom Netzwerk aus auf diese Maschine einloggen möchten.
/etc/init.d/portmap	Startet den Portmapper, der benötigt wird, um RPC-Server verwenden zu können, wie z. B. einen NFS-Server.
/etc/init.d/nfsserver	Startet den NFS-Server.
/etc/init.d/sendmail	Kontrolliert den sendmail-Prozess.
/etc/init.d/ypserv	Startet den NIS-Server.
/etc/init.d/ypbind	Startet den NIS-Client.

Tabelle 12.11: *Einige Startup-Skripten der Netzwerkprogramme*

Routing unter SuSE Linux

Ab SuSE Linux 8.0 wird die Routing-Tabelle in den Konfigurationsdateien `/etc/sysconfig/network/routes` und `/etc/sysconfig/network/ifroute-*` eingestellt.

In der Datei `/etc/sysconfig/network/routes` können alle statischen Routen eingetragen werden, die für die verschiedenen Aufgaben eines Systems benötigt werden könnten: Route zu einem Rechner, Route zu einem Rechner über ein Gateway und Route zu einem Netzwerk.

Für alle Interfaces, die individuelles Routing benötigen, kann dies jeweils in einer eigenen Datei pro Interface definiert werden: `/etc/sysconfig/network/ifroute-*`. Für das Zeichen '`*`' muss die Interface-Bezeichnung eingesetzt werden. Die Einträge können folgendermaßen aussehen:

```
DESTINATION           GATEWAY NETMASK   INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION           GATEWAY PREFIXLEN INTERFACE [ TYPE ] [ OPTIONS ]
DESTINATION/PREFIXLEN GATEWAY -         INTERFACE [ TYPE ] [ OPTIONS ]
```

Falls GATEWAY, NETMASK, PREFIXLEN oder INTERFACE nicht angegeben werden, muss an ihrer Stelle das Zeichen '`-`' gesetzt werden. Die Einträge TYPE und OPTIONS können schlicht entfallen.

- In der ersten Spalte steht das Ziel einer Route. Dabei kann dort die IP-Adresse eines Netzes oder Rechners oder bei *erreichbaren* Nameservern auch der voll qualifizierte Name eines Netzes oder eines Rechners stehen.
- Die zweite Spalte enthält entweder das Default-Gateway oder ein Gateway, hinter dem ein Rechner oder Netzwerk erreichbar ist.
- Die dritte Spalte enthält die Netzmaske für Netzwerke oder Rechner hinter einem Gateway. Für Rechner hinter einem Gateway lautet die Maske z. B. `255.255.255.255`.
- Die letzte Spalte ist nur für die am lokalen Rechner angeschlossenen Netzwerke (Loopback, Ethernet, ISDN, PPP, ...) wichtig. Hier muss der Name des Devices eingetragen werden.

DNS – Domain Name Service

DNS (engl. *Domain Name Service*) wird benötigt, um die Domain- und Rechnernamen in IP-Adressen aufzulösen. Bevor Sie einen eigenen Nameserver einrichten, sollten Sie die allgemeinen Informationen zu DNS im Abschnitt 12 auf Seite 277 lesen.

Nameserver BIND starten

Der Nameserver BIND ist auf SuSE Linux bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann.

Hat man bereits eine funktionsfähige Internetverbindung und trägt in der `/etc/resolv.conf` als Nameserver 127.0.0.1 für localhost ein, hat man in der Regel schon eine funktionierende Namensauflösung, ohne dass man den DNS des Providers kennt. BIND führt so die Namensauflösung über die Root-Nameserver durch, was aber merklich langsamer ist. Normalerweise sollte man den DNS des Providers mit seiner IP-Adresse in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` eintragen, um eine effektive und sichere Namensauflösung zu erhalten. Funktioniert das soweit, läuft der Nameserver als reiner „Caching-only"-Nameserver. Erst wenn man ihm eigene Zonen bereitstellt, wird er ein richtiger DNS werden. Ein einfaches Beispiel dafür, findet man im Doku-Verzeichnis: `/usr/share/doc/packages/bind8/sample-config`.

Man sollte allerdings keine offizielle Domain aufsetzen, solange man diese nicht von der zuständigen Institution – für '.de' ist das die DENIC eG – zugewiesen bekommen hat. Auch wenn man eine eigene Domain hat, diese aber vom Provider verwaltet wird, sollte man diese besser nicht verwenden, da BIND sonst keine Anfragen für diese Domain mehr forwarden würde und so z. B. der Webserver beim Provider für die eigene Domain nicht mehr erreichbar wäre.

Um den Nameserver zu starten gibt man auf der Kommandozeile (als root)

```
rcnamed start
```

ein. Erscheint rechts in grün „done", ist der `named`, so heißt der Nameserver-Prozess, erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit des Nameservers sofort testen, indem man das Programm `nslookup` verwendet. Als Default Server muss localhost mit der Adresse 127.0.0.1 angezeigt werden. Sollte das nicht der Fall sein, steht wahrscheinlich in der `/etc/resolv.conf` ein falscher Nameserver oder diese Datei existiert gar nicht. Für einen ersten Test gibt man auf dem Prompt von

`nslookup` „127.0.0.1“ ein, das sollte immer funktionieren; erhält man stattdessen eine Fehlermeldung „No response from server“ oder ähnlich, dann sollte man mit folgendem Kommando überprüfen, ob der `named` überhaupt läuft

```
rcnamed status
```

Falls der Nameserver nicht startet oder ein fehlerhaftes Verhalten zeigt, findet man die Ursache in den meisten Fällen in „/var/log/messages“ protokolliert.

Hat man eine Wählverbindung, muss man beachten, dass BIND8 beim Starten die Root-Nameserver überprüfen will. Gelingt ihm das nicht, weil keine Internetverbindung zustande kommt, kann das dazu führen, dass überhaupt keine DNS-Anfragen außer für lokal definierte Zonen aufgelöst werden können. BIND9 verhält sich da anders, benötigt aber ein Mehrfaches an Ressourcen im Vergleich zu BIND8.

Um den Nameserver des Providers, oder einen eigenen, den man schon im eigenen Netz laufen hat, als „forwarder“ zu verwenden, trägt man diesen oder auch mehrere, im Abschnitt `options` unter `forwarders` ein; vgl. Beispiel 21.

```
options {
         directory "/var/lib/named";
         forwarders { 10.11.12.13; 10.11.12.14; };
         listen-on { 127.0.0.1; 192.168.0.99; };
         allow-query { 127/8; 192.168.0/24; };
         notify no;
        };
```

Datei 21: *Forwarding-Optionen in* `named.conf`

Die im Beispiel verwendeten IP-Adressen sind willkürlich gewählt und müssen entsprechend den eigenen Gegebenheiten eingetragen werden.

Nach den `options` folgen dann die Einträge für die Zonen, die Einträge für „localhost“, „0.0.127.in-addr.arpa“, sowie „.“ vom „type hint“ sollten mindestens immer vorhanden sein. Die zugehörigen Dateien müssen nicht verändert werden, da sie so funktionieren wie sie sind. Beachten muss man auch, dass nach jedem Eintrag ein „;“ steht und die geschweiften Klammern korrekt gesetzt sind. Hat man nun Änderungen an der Konfigurationsdatei `/etc/named.conf` oder an den Zonen-Dateien vorgenommen, muss man BIND dazu bringen diese neu einzulesen. Das gelingt mit dem Kommando

rcnamed reload. Alternativ kann man den Nameserver auch komplett neu starten, durch den Befehl rcnamed restart. Fehlt nur noch das Kommando, um den Nameserver wieder zu beenden: rcnamed stop.

Die Konfigurationsdatei /etc/named.conf

Alle Einstellungen zum Nameserver BIND8 bzw. BIND9 sind in der Datei /etc/named.conf vorzunehmen. Die Zonendaten selbst, die Rechnernamen, IP-Adressen usw. für die zu verwaltenden Domains, sind in separaten Dateien im Verzeichnis /var/lib/named abzulegen, dazu aber unten mehr.

Die /etc/named.conf unterteilt sich grob in zwei Bereiche, zum einen der Abschnitt options für allgemeine Einstellungen und zum anderen die zone-Einträge für die einzelnen Domains. Außerdem kann man noch einen Bereich logging, sowie Einträge vom Typ acl definieren. Kommentarzeilen beginnen mit einem '#'-Zeichen, alternativ ist '//' auch erlaubt.

Eine minimalistische /etc/named.conf stellt Beispiel 22 dar.

```
options {
        directory "/var/lib/named";
        forwarders { 10.0.0.1; };
        notify no;
};

zone "localhost" in {
       type master;
       file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "127.0.0.zone";
};

zone "." in {
        type hint;
        file "root.hint";
};
```

Datei 22: *Minimalistische Datei /etc/named.conf*

Dieses Beispiel funktioniert für Bind8 und Bind9 gleichermaßen, da keine speziellen Optionen verwendet werden, die nur von einer Version verstanden werden. Bind9 akzeptiert alle Bind8-Konfigurationen und vermerkt allenfalls beim Start, wenn eine Option nicht implementiert ist. Spezielle Bind9-Optionen werden vom Bind8 aber nicht unterstützt.

Die wichtigsten Konfigurationsoptionen im Abschnitt options

directory "/var/lib/named"; gibt das Verzeichnis an, in dem der BIND die Dateien mit den Zonendaten findet,

forwarders { 10.0.0.1; }; verwendet man, um den oder die Nameserver (meist des Providers) anzugeben, an den oder die DNS-Anfragen weitergereicht werden, die nicht direkt beantwortet werden können.

forward first; bewirkt, dass die DNS-Anfragen zu erst geforwarded werden, bevor versucht wird diese über die Root-Nameserver aufzulösen. Anstelle von `forward first` kann man auch `forward only` schreiben, dann werden alle Anfragen weitergeleitet und die Root-Nameserver werden gar nicht mehr angesprochen. Das kann für Firewall-Konfigurationen sinnvoll sein.

listen-on port 53 { 127.0.0.1; 192.168.0.1; }; sagt dem BIND, auf welchen Netzwerkinterfaces und welchem Port er auf Anfragen der Clients horcht. Die Angabe `port 53` kann man sich dabei sparen, da 53 ohnehin der Standardport ist. Lässt man diesen Eintrag komplett weg, werden standardmäßig alle Interfaces verwendet

query-source address * port 53; Dieser Eintrag kann notwendig sein, wenn eine Firewall die externen DNS-Abfragen blockiert. So wird BIND dazu gebracht, Anfragen nach außen von Port 53 aus und nicht von den hohen Port's > 1024 zu stellen.

allow-query { 127.0.0.1; 192.168.1/24; }; bestimmt die Netze aus denen Clients DNS-Anfragen stellen dürfen. Das `/24` ist dabei eine Kurzschreibweise für die Netzmaske, in diesem Fall 255.255.255.0.

allow-transfer { ! *; }; regelt welche Rechner Zonentransfers anfordern dürfen, dieses Beispiel unterbindet sie, aufgrund des `! *` komplett. Ohne diesen Eintrag können Zonentransfers ohne Einschränkungen von überall angefordert werden.

statistics-interval 0; Ohne diesen Eintrag produziert Bind8 stündlich mehrere Zeilen Statistikmeldungen in `/var/log/messages`. Die Angabe von 0 bewirkt, dass diese komplett unterdrückt werden, ansonsten kann man hier die Zeit in Minuten angeben.

cleaning-interval 720; Diese Option legt fest, in welchem Zeitabstand Bind8 seinen Cache aufräumt. Die Aktivität führt jedes Mal zu einem Eintrag in /var/log/messages. Die Zeitangabe erfolgt in Minuten. Voreingestellt sind 60 Minuten.

interface-interval 0; Bind8 durchsucht regelmäßig die Netzwerkschnittstellen nach neuen oder nicht mehr vorhandenen Interfaces. Setzt man diesen Wert auf `0`, so wird darauf verzichtet und Bind8 lauscht nur auf den beim Start gefundenen Interfaces. Alternativ kann man das Intervall in Minuten angeben. Voreingestellt sind 60 Minuten.

notify no; Das `no` bewirkt, dass keine anderen Nameserver benachrichtigt werden, wenn an den Zonendaten Änderungen vorgenommen werden oder der Nameserver neu gestartet wird.

Der Konfigurationsabschnitt Logging

Was und wie wohin mitprotokolliert wird, kann man beim Bind8 recht vielseitig konfigurieren. Normalerweise sollte man mit den Voreinstellungen zufrieden sein können. Beispiel 23 zeigt die einfachste Form so eines Eintrages und unterdrückt das „Logging" komplett

```
logging {
        category default { null; };
};
```

Datei 23: *Logging wird unterdrückt*

Aufbau der Zonen-Einträge

Nach `zone` wird der Name der zu verwaltenden Domain angegeben, hier willkürlich `meine-domain.de` gefolgt von einem `in` und einem in geschweiften Klammern gesetzten Block zugehöriger Optionen; vgl. Datei 24.

```
zone "meine-domain.de" in {
       type master;
       file "meine-domain.zone";
       notify no;
};
```

Datei 24: *Zone-Eintrag für meine-domain.de*

Will man eine „Slave-Zone“ definieren, ändert sich nur der `type` auf `slave` und es muss ein Nameserver angegeben werden, der diese Zone als `master` verwaltet (kann aber auch ein „slave“ sein); vgl. Datei 25.

```
zone "andere-domain.de" in {
        type slave;
        file "slave/andere-domain.zone";
        masters { 10.0.0.1; };
};
```

Datei 25: *Zone-Eintrag für andere-domain.de*

Die Optionen:

type master; Das `master` legt fest, dass diese Zone auf diesem Nameserver verwaltet wird. Das setzt eine sauber erstellte Zonendatei voraus.

type slave; Diese Zone wird von einem anderen Nameserver transferiert. Muss zusammen mit `masters` verwendet werden.

type hint; Die Zone `.` vom Typ `hint` wird für die Angabe der Root-Nameserver verwendet. Diese Zonendefinition kann man unverändert lassen.

file „meine-domain.zone“ oder file „slave/andere-domain.zone“; Dieser Eintrag gibt die Datei an, in der die Zonendaten für die Domain eingetragen sind. Bei einem `slave` braucht die Datei nicht zu existieren, da ihr Inhalt von einem anderen Nameserver geholt wird. Um Master- und Slave-Dateien auseinander zu halten, gibt man für die Slave-Dateien das Verzeichnis `slave` an.

masters { 10.0.0.1; }; Diesen Eintrag braucht man nur für Slave-Zonen und er gibt an, von welchem Nameserver die Zonendatei transferiert werden soll.

allow-update { ! *; }; diese Option regelt den Schreibzugriff von extern auf die Zonendaten. Damit wäre es Clients möglich, sich selbst im DNS einzutragen, was aus Sicherheitsgründen nicht wünschenswert ist. Ohne diesen Eintrag, sind Zonen-Updates generell untersagt, dieses Beispiel würde daran auch nichts ändern, da `! *` ebenfalls alles verbietet.

Aufbau der Zonendateien

Man benötigt zwei Arten von Zonen-Dateien, die einen dienen dazu, einem Rechnernamen die IP-Adresse zu zuordnen und die anderen gehen den umgekehrten Weg und liefern zu einer gegebenen IP-Adresse den Rechnernamen.

Eine wichtige Bedeutung hat der '.' in den Zonendateien. Werden Rechnernamen, ohne abschließenden '.' angegeben, wird immer die Zone ergänzt. Man muss also komplette Rechnernamen, die bereits mit vollständiger Domain angegeben wurden, mit einem '.' abschließen, damit die Domain nicht noch einmal dran gehängt wird. Ein fehlender Punkt oder einer an der falschen Stelle, dürfte die häufigste Fehlerursache bei der Konfiguration von Nameservern sein.

Den ersten Fall betrachten wir an der Zonen-Datei `welt.zone`, die für die Domain `welt.all` zuständig ist; vgl. Datei 26.

```
1.  $TTL 2D
2.  welt.all.    IN SOA      gateway  root.welt.all. (
3.               2001040901  ; serial
4.               1D          ; refresh
5.               2H          ; retry
6.               1W          ; expiry
7.               2D )        ; minimum
8.
9.               IN NS       gateway
10.              IN MX       10 sonne
11.
12. gateway      IN A        192.168.0.1
13.              IN A        192.168.1.1
14. sonne        IN A        192.168.0.2
15. mond         IN A        192.168.0.3
16. erde         IN A        192.168.1.2
17. mars         IN A        192.168.1.3
```

Datei 26: *Datei* `/var/lib/named/welt.zone`

Zeile 1: `$TTL` definiert die Standard-TTL, die für alle Einträge in dieser Datei gilt, hier 2 Tage (2D = 2 days). TTL bedeutet hier „time to live", zu deutsch Gültigkeitsdauer.

Zeile 2: Hier beginnt der `SOA control record`:

- An erster Stelle steht hier der Name der zu verwaltenden Domain `welt.all`, diese ist mit einem '.' abgeschlossen, da ansonsten die Zone noch einmal angehängt würde. Alternativ kann man hier ein `'@'` schreiben, dann wird die Zone dem zugehörigen Eintrag in der `/etc/named.conf` entnommen.
- Nach dem `IN SOA` steht der Name des Nameservers, der als Master für diese Zone zuständig ist. In diesem Fall wird der Name `gateway` zu `gateway.welt.all` ergänzt, da er nicht mit einem `'.'` abgeschlossen ist.
- Danach folgt eine E-Mail-Adresse, der für diesen Nameserver zuständigen Person. Da das `'@'`-Zeichen bereits eine besondere Bedeutung hat, ist hier stattdessen einfach ein `'.'` einzutragen, für `root@welt.all` schreibt man hier folglich `root.welt.all.`. Den `'.'` am Ende darf man hier nicht vergessen, da sonst die Zone noch angehängt würde.
- Am Ende folgt eine `'('`, um die folgenden Zeilen, bis zur `')'` mit in den SOA-Record einzuschließen.

Zeile 3: Die `serial number` ist eine willkürliche Zahl, die bei jeder Änderung an dieser Datei erhöht werden sollte. Sie wird benötigt, um sekundäre Nameserver (Slave-Server) über Änderungen zu informieren. Eingebürgert hat sich dafür eine zehnstellige Zahl aus Datum und fortlaufender Nummer in der Form JJJJMMTTNN.

Zeile 4: Die `refresh rate` gibt das Zeitintervall an, in dem Sekundär-Nameserver die `serial number` der Zone überprüfen. In diesem Fall 1 Tag (1D = 1 day).

Zeile 5: Die `retry rate` gibt den Zeitabstand an, in dem ein sekundärer Nameserver, im Fehlerfall versucht den primären Server erneut zu kontaktieren. Hier 2 Stunden (2H = 2 hours).

Zeile 6: Die `expiration time` gibt den Zeitraum an, nachdem ein sekundärer Nameserver die gecacheten Daten verwirft, wenn er keinen Kontakt zum primären Server mehr bekommen hat. Hier ist das eine Woche (1W = 1 week).

Zeile 7: Die `minimum time to live` sagt aus, wie lange die Ergebnisse von DNS-Anfragen von anderen Servern gecached werden dürfen, bevor sie ihre Gültigkeit verlieren und neu angefragt werden müssen.

Zeile 9: Das `IN NS` gibt den Nameserver an, der für diese Domain zuständig ist. Auch hier gilt, dass `gateway` wieder zu `gateway.welt.all`

ergänzt wird, weil es nicht mit einem `'.'` abgeschlossen ist. Es kann mehrere Zeilen dieser Art geben, eine für den primären und jeweils eine für jeden sekundären Nameserver. Ist für diese Zone `notify` in der `/etc/named.conf` nicht auf `no` gesetzt, werden alle hier aufgeführten Nameserver über Änderungen der Zonendaten informiert.

Zeile 10: Der MX-Record gibt den Mailserver an, der für die Domain `welt.all` die Mails annimmt und weiterverarbeitet oder weiterleitet. In diesem Beispiel ist das der Rechner `sonne.welt.all`. Die Zahl vor dem Rechnernamen ist der Präferenz-Wert, gibt es mehrere MX-Einträge, wird zuerst der Mailserver mit dem kleinsten Wert genommen und falls die Auslieferung an diesen scheitert, wird der mit dem nächst höheren Wert versucht.

Zeile 12-17: Das sind jetzt die eigentlichen Adress-Records, in denen den Rechnernamen eine oder mehrere IP-Adressen zugeordnet werden. Die Namen stehen hier ohne abschließenden `.`, da sie ohne angehängte Domain eingetragen sind und alle um `welt.all` ergänzt werden dürfen. Dem Rechner `gateway` sind zwei IP-Adressen zugeordnet, da er über zwei Netzwerkkarten verfügt.

Für die Rückwärts-Auflösung (reverse lookup) von IP-Adressen in Rechnernamen wird die Pseudo-Domain `in-addr.arpa` zu Hilfe genommen. Diese wird dazu an den in umgedrehter Reihenfolge geschriebenen Netzanteil angehängt. Aus `192.168.1` wird dann `1.168.192.in-addr.arpa`; vgl. 27.

```
1. $TTL 2D
2. 1.168.192.in-addr.arpa. IN SOA gateway.welt.all. root.welt.all. (
3.                         2001040901      ; serial
4.                         1D              ; refresh
5.                         2H              ; retry
6.                         1W              ; expiry
7.                         2D )            ; minimum
8.
9.                         IN NS           gateway.welt.all.
10.
11. 1                      IN PTR          gateway.welt.all.
12. 2                      IN PTR          erde.welt.all.
13. 3                      IN PTR          mars.welt.all.
```

Datei 27: *Umgekehrte Adress-Auflösung*

Zeile 1: $TTL definiert die Standard-TTL, die hier für alle Einträge gilt.

Zeile 2: Der 'revers lookup' soll mit dieser Datei für das Netz 192.168.1.0 ermöglicht werden. Da die Zone hier '1.168.192.in-addr.arpa' heißt, will man dies natürlich nicht an die Rechnernamen anhängen, deshalb sind diese alle komplett mit Domain und abschließendem '.' eingetragen. Der Rest entspricht dem, was im vorangegangenen Beispiel für "welt.all", bereits beschrieben wurde.

Zeile 3-7: Siehe vorangegangenes Beispiel für "welt.all".

Zeile 9: Diese Zeile gibt auch hier wieder den Nameserver an, der für diese Zone zuständig ist, diesmal wird aber der Name komplett mit Domain und abschließendem '.' hier eingetragen.

Zeile 11-13: Das sind die Pointer-Records, die zu einer IP-Adresse auf den zugehörigen Rechnernamen zeigen. Hier steht am Anfang der Zeile nur die letzte Stelle der IP-Adresse, ohne abschließenden '.'. Wird jetzt die Zone daran angehängt und man denkt sich das '.in-addr.arpa' weg, hat man die komplette IP-Adresse in verdrehter Reihenfolge.

Die Zonendateien sind in dieser Form für Bind8 und Bind9 gleichermaßen verwendbar. Auch Zonentransfers zwischen den verschiedenen Versionen sollten normalerweise kein Problem darstellen.

Weitere Informationen

- Dokumentation zum Paket `bind8`: `file:/usr/share/doc/packages/bind8/html/index.html`.
- Eine Beispielkonfiguration findet man unter: `/usr/share/doc/packages/bind8/sample-config`
- Manual-Page von `named` (`man 8 named`), in der die einschlägigen RFCs genannt werden, sowie besonders die Manual-Page von `named.conf` (`man 5 named.conf`).

NIS – Network Information Service

Sobald mehrere Unix-Systeme in einem Netzwerk auf gemeinsame Ressourcen zugreifen wollen, muss sichergestellt sein, dass Benutzer- und Gruppenkennungen auf allen Rechnern miteinander harmonieren. Das Netzwerk soll für den Anwender transparent sein. Egal welcher Rechner, der Anwender findet immer die gleiche Umgebung vor. Möglich wird dies durch die Dienste NIS und NFS. NFS dient der Verteilung von Dateisystemen im Netz und wird in Abschnitt *NFS – verteilte Dateisysteme* auf Seite 312 beschrieben.

NIS (engl. *Network Information Service*) kann als Datenbankdienst verstanden werden, der Zugriff auf Informationen aus den Dateien `/etc/passwd`, `/etc/shadow` oder `/etc/group` netzwerkweit ermöglicht. NIS kann auch für weitergehende Aufgaben eingesetzt werden (z. B. für `/etc/hosts` oder `/etc/services`). Darauf soll hier jedoch nicht im Detail eingegangen werden. Für NIS wird vielfach synonym der Begriff `'YP'` verwendet. Dieser leitet sich ab von den *yellow pages*, also den *gelben Seiten* im Netz.

NIS-Master- und -Slave-Server

Zur Installation wählen Sie in YaST2 'Netzwerk/Erweitert' und dort 'NIS-Server konfigurieren'.

Wenn in Ihrem Netzwerk bisher noch kein NIS-Server existiert, müssen Sie in der nächsten Maske den Punkt 'NIS Master Server einrichten' aktivieren. Falls Sie schon einen NIS-Server (also einen „Master“) haben, können Sie (z. B. wenn Sie ein neues Subnetz einrichten) einen NIS Slave Server hinzufügen. Als Erstes wird die Konfiguration des Master-Servers erläutert. In der ersten Konfigurationsmaske (Abb. 12.4 auf der nächsten Seite) geben Sie oben den Domainnamen ein. In der Checkbox darunter können Sie festlegen, ob der Rechner auch ein NIS-Client werden soll, also ob sich darauf auch User einloggen können, die dann ebenfalls die Daten von dem NIS-Server erhalten.

Wollen Sie später weitere NIS-Server („Slave-Server“) in Ihrem Netzwerk einrichten, müssen Sie die Box 'Aktiver Slave-Server für NIS vorhanden' aktivieren. Zusätzlich sollten Sie dann auch die 'Schnelle Map-Verteilung' aktivieren, die bewirkt, dass die Datenbankeinträge sehr schnell vom Master auf die Slave-Server übertragen werden.

Wollen Sie den Nutzern in Ihrem Netzwerk erlauben, dass sie Ihre Passwörter ändern können (mit dem Befehl `yppasswd`, also nicht nur die lokalen, sondern die, die auf dem NIS-Server abgelegt sind), können Sie das hier ebenfalls aktivieren. Dann werden auch die Checkboxen 'Ändern des GECOS-Eintrags zulassen' und 'Ändern des SHELL-Eintrags zulassen' aktiv. „GECOS“ bedeutet, der User kann auch seine Namens- und Adresseinstellungen

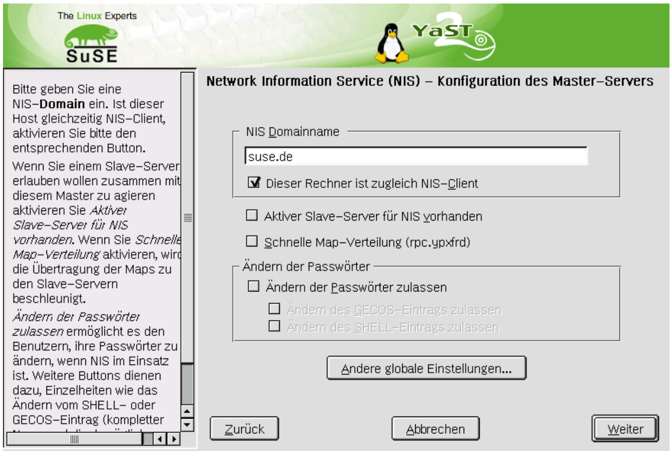


Abbildung 12.4: *YaST2: NIS-Server Konfigurationstool*

ändern (mit dem Befehl ypchfn). „SHELL" heißt, er darf auch seine standardmäßig eingetragene Shell ändern (mit dem Befehl ypchsh, z. B. von bash zu sh).

Unter 'Andere globale Einstellungen...' erscheint ein Menü (Abb. 12.5 auf der nächsten Seite), in dem man das Standardverzeichnis (/etc) ändern kann. Zusätzlich kann man hier noch Passwörter und Gruppen zusammenführen. Die Einstellung sollte man auf 'Ja' belassen, damit die jeweiligen Dateien (/etc/passwd und /etc/shadow bzw. /etc/group und /etc/gshadow) aufeinander abgestimmt werden. Zusätzlich kann noch die jeweils kleinste Benutzer- und Gruppenkennummer festgelegt werden. Mit 'OK' kommen Sie wieder in die vorige Maske zurück. Klicken Sie nun auf 'Weiter'.

Haben Sie vorher 'Aktiver Slave-Server für NIS vorhanden' aktiviert, müssen Sie nun die Namen der Rechner angeben, die als Slaves fungieren sollen. Legen Sie die Namen fest und gehen Sie auf 'Weiter'. Das folgende Menü erreichen Sie auch direkt, wenn Sie vorher die Einstellung für die Slave-Server nicht aktiviert haben. Nun können die „Maps", d. h. die Teildatenbanken, die vom NIS-Server auf den jeweiligen Client übertragen werden sollen. Die Voreinstellungen hier sind für die meisten Fälle sehr sinnvoll. Daher sollten Sie im Normalfall hier nichts ändern. Falls Sie hier doch Änderungen vornehmen wollen, sollten Sie sich in der Materie sehr gut auskennen.

Mit 'Weiter' kommen Sie in den letzten Dialog, in dem festgelegt werden kann, welche Netzwerke Anfragen an den NIS-Server stellen dürfen (siehe

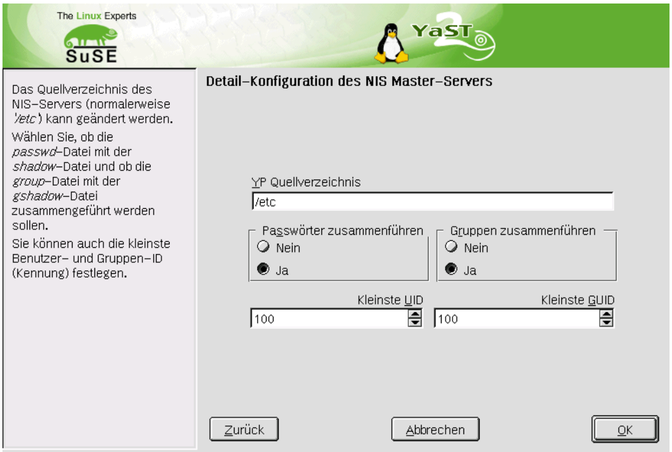


Abbildung 12.5: *YaST2: NIS-Server: Verzeichnis ändern und Dateien synchronisieren*

Abb. 12.6 auf der nächsten Seite). Normalerweise wird das Ihr Firmennetzwerk sein. Dann sollten die beiden Eintragungen

```
255.0.0.0 127.0.0.0
0.0.0.0 0.0.0.0
```

hier stehen. Die erste erlaubt Verbindungen vom eigenen Rechner, die zweite ermöglicht allen Rechnern, die Zugriff auf das Netzwerk haben, Anfragen an den Server.

Das NIS-Client-Modul im YaST2

Mit diesem Modul können Sie sehr einfach den NIS-Client konfigurieren. Im Startfenster geben Sie an, dass Sie NIS benutzen möchten. Im folgenden Dialog können Sie dann die NIS-Domain und die IP-Nummer des NIS-Servers angeben. Mit der 'Broadcast'-Checkbox ermöglichen Sie die Suche nach einem NIS-Server im Netzwerk, wenn der angegebene Server nicht antwortet. Sie haben auch die Möglichkeit, multiple Domains mit einer Default-Domain anzugeben. Für die einzelnen Domains könenn Sie wiederum mit 'Hinzufügen' mehrere Server einschließlich Broadcast-Funktion angeben.

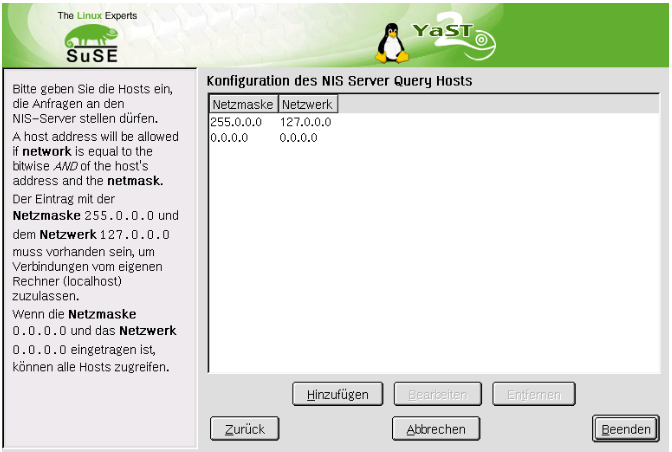


Abbildung 12.6: *YaST2: NIS-Server: Festlegung der Anfrageerlaubnis*

Manuelles Einrichten eines NIS-Clients

Im Paket `ypbind`, befinden sich alle notwendigen Programme zum Einrichten eines NIS-Clients. Folgende Schritte sind notwendig:

- Setzen Sie die NIS-Domain in der Datei `/etc/defaultdomain`
  Der NIS-Domainname ist nicht zu verwechseln mit dem DNS--Domainnamen. Diese können gleich lauten, haben jedoch grundsätzlich nichts miteinander zu tun!

- Der Name des NIS-Server wird in der Datei `/etc/yp.conf` eingetragen:

  ```
  ypserver 192.168.0.1
  ```

- Der Name des NIS-Servers (z. B. `sonne.kosmos.all`) muss über `/etc/hosts` auflösbar sein.

- NIS wird über RPC (engl. *Remote Procedure Calls*) realisiert, deshalb ist es Bedingung, dass der RPC-Portmapper läuft. Gestartet wird dieser Server vom Skript `/etc/init.d/portmap`.

- Ergänzen der Einträge in `/etc/passwd` und `/etc/group`. Damit nach dem Durchsuchen der lokalen Dateien eine Anfrage beim NIS-Server

gemacht wird, müssen die entsprechenden Dateien durch eine Zeile, die mit einem Pluszeichen (`'+'`) beginnt, ergänzt werden.

- NIS erlaubt es, eine Menge weiterer Optionen in der Datei `/etc/sysconfig/ypbind` zu aktivieren.
- Der letzte Schritt des Aufsetzens des NIS-Clients besteht aus dem Start des Programmes ypbind und damit des eigentlichen NIS-Clients.
- Entweder muss nun das System neu gestartet werden oder die benötigten Dienste werden durch folgende Befehle neu gestartet:

```
erde: # rcnetwork restart
erde: # rcypbind restart
```

NFS – verteilte Dateisysteme

Wie bereits in Abschnitt *NIS – Network Information Service* auf Seite 307 erwähnt, dient NFS neben NIS dazu, ein Netzwerk für Anwender transparent zu machen. Durch NFS lassen sich Dateisysteme im Netz verteilen. Unabhängig davon, an welchem Rechner im Netz ein Anwender arbeitet, findet er so stets die gleiche Umgebung vor.

Wie NIS ist auch NFS ein asymmetrischer Dienst. Es gibt NFS-Server und NFS-Clients. Allerdings kann ein Rechner beides sein, d. h. gleichzeitig Dateisysteme dem Netz zur Verfügung stellen („exportieren“) und Dateisysteme anderer Rechner mounten („importieren“). Im Regelfall jedoch benutzt man dafür Server mit großer Festplattenkapazität, deren Dateisysteme von Clients gemountet werden.

Importieren von Dateisystemen mit YaST2

Jeder Benutzer (der die Rechte dazu erteilt bekommt), kann NFS-Verzeichnisse von NFS-Servern in seinen eigenen Dateibaum einhängen. Dies läßt sich am einfachsten mit dem Modul 'NFS-Client' in YaST2 erledigen. Dort muss lediglich der Hostname des als NFS-Server fungierenden Rechners eingetragen werden, das Verzeichnis, das von dem Server exportiert wird und den Mountpunkt, unter dem es auf dem eigenen Computer eingehängt werden soll. Wählen Sie dazu im ersten Dialogfenster 'Hinzufügen' und tragen Sie dann die genannten Angaben ein (s. Abb. 12.7).



Abbildung 12.7: *Konfiguration des NFS-Clients*

Manuelles Importieren von Dateisystemen

Dateisysteme von einem NFS-Server zu importieren, ist sehr einfach. Einzige Voraussetzung ist, dass der RPC-Portmapper gestartet wurde. Das Starten dieses Servers wurde bereits im Zusammenhang mit NIS besprochen (siehe Abschnitt *Manuelles Einrichten eines NIS-Clients* auf Seite 310). Ist diese Voraussetzung erfüllt, können fremde Dateisysteme, sofern sie von den entsprechenden Maschinen exportiert werden, analog zu lokalen Platten mit dem Befehl `mount` in das Dateisystem eingebunden werden. Die Syntax ist wie folgt:

`mount -t nfs` ⟨*Rechner*⟩:⟨*Remote-Pfad*⟩ ⟨*Lokaler-Pfad*⟩

Sollen also z. B. die Benutzerverzeichnisse vom Rechner `sonne` importiert werden, so kann dies mit folgendem Befehl erreicht werden:

```
erde:~ #  mount -t nfs sonne:/home /home
```

Exportieren von Dateisystemen mit YaST2

Mit YaST2 können Sie sehr schnell einen Rechner Ihres Netzwerks zu einem NFS-Server machen. Das ist ein Server, der Verzeichnisse und Dateien für alle Rechner, denen Sie Zugang gewähren, bereitstellt. Viele Anwendungsprogramme können so z. B. für Mitarbeiter zur Verfügung gestellt werden, ohne dass sie lokal auf deren Rechnern installiert werden müssen.

Zur Installation wählen Sie in YaST2 'Netzwerk/Erweitert' und dort 'NFS-Server' (Abb. 12.8 auf der nächsten Seite).

Im nächsten Schritt aktivieren Sie 'NFS-Server starten' und klicken auf 'Weiter'

Jetzt ist nur noch ein Schritt zu tun: Sie müssen im oberen Feld die Verzeichnisse eintragen, die exportiert werden sollen und im unteren die Rechner Ihres Netzwerks, die darauf Zugriff erhalten (Abb. 12.9 auf Seite 315). Zu den Rechnern sind jeweils vier Optionen einstellbar, ⟨*single host*⟩, ⟨*netgroups*⟩, ⟨*wildcards*⟩ und ⟨*IP networks*⟩. Nähere Erläuterungen zu diesen Optionen finden Sie in den manpages zu Paket `exports` (`man exports`).

Mit 'Beenden' schließen Sie die Konfiguration ab.

Manuelles Exportieren von Dateisystemen

Auf einem NFS-Server müssen die folgenden Netzwerkserver gestartet werden:

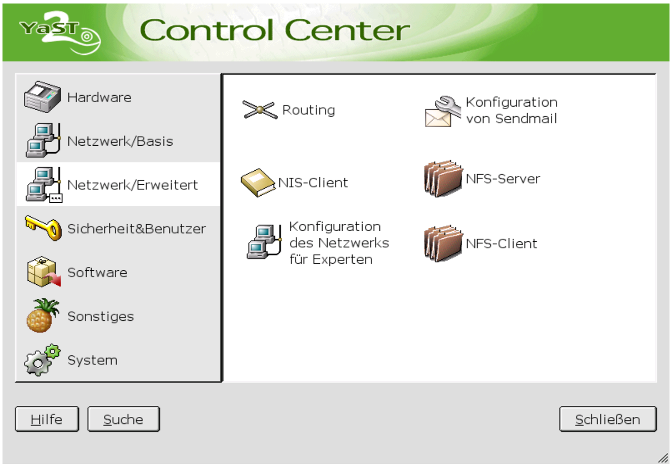


***Abbildung 12.8:** YaST2: NFS-Server Konfigurationstool*

- RPC-Portmapper (portmap)
- RPC-Mount-Daemon (rpc.mountd)
- RPC-NFS-Daemon (rpc.nfsd)

Diese werden beim Hochfahren des Systems von den Skripten /etc/init.d/portmap und /etc/init.d/nfsserver gestartet.

Neben dem Start dieser Daemonen muss noch festgelegt werden, welche Dateisysteme an welche Rechner exportiert werden sollen. Dies geschieht in der Datei `/etc/exports`.

Je Verzeichnis, das exportiert werden soll, wird eine Zeile für die Information benötigt, welche Rechner wie darauf zugreifen dürfen. Alle Unterverzeichnisse eines exportierten Verzeichnisses werden ebenfalls automatisch exportiert. Die berechtigten Rechner werden üblicherweise mit ihren Namen (inklusive Domainname) angegeben, es ist aber auch möglich, mit den Jokerzeichen `'*'` und `'?'` zu arbeiten, die die aus der bash bekannte Funktion haben. Wird kein Rechnername angegeben, hat jeder Rechner die Erlaubnis, auf dieses Verzeichnis (mit den angegebenen Rechten) zuzugreifen.

Die Rechte, mit denen das Verzeichnis exportiert wird, werden in einer von Klammern umgebenen Liste nach dem Rechnernamen angegeben. Die wichtigsten Optionen für die Zugriffsrechte sind in der folgenden Tabelle beschrieben.

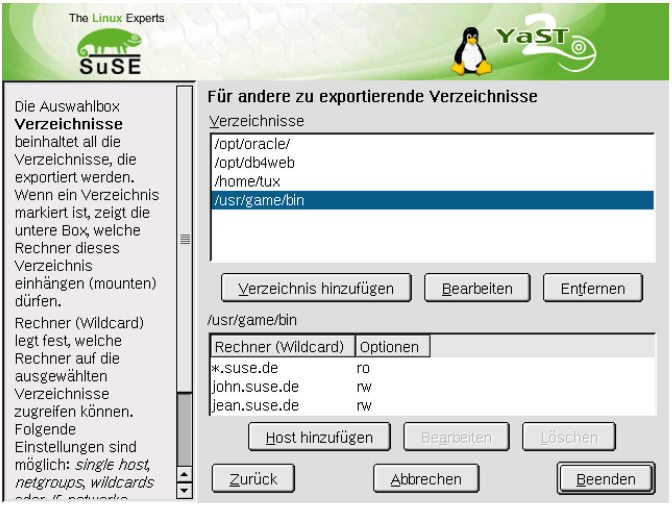


Abbildung 12.9: *YaST2: NFS-Server: Exportverzeichnisse und Hosts eintragen*

Optionen	**Bedeutung**
ro	Dateisystem wird nur mit Leserechten exportiert (Vorgabe).
rw	Dateisystem wird mit Schreib- und Leserechten exportiert.
root_squash	Diese Option bewirkt, dass der Benutzer `root` des angegebenen Rechners keine für `root` typischen Sonderrechte auf diesem Dateisystem hat. Erreicht wird dies, indem Zugriffe mit der User-ID `0` auf die User-ID `65534 (-2)` umgesetzt werden. Diese User-ID sollte dem Benutzer `nobody` zugewiesen werden (Vorgabe).
no_root_squash	Rootzugriffe nicht umsetzen; Rootrechte bleiben also erhalten.

Tabelle 12.12: *Fortsetzung auf der nächsten Seite...*

link_relative	Umsetzen von absoluten, symbolischen Links (solche, die mit '/' beginnen) in eine entsprechende Folge von '../'. Diese Option ist nur dann sinnvoll, wenn das gesamte Dateisystem eines Rechners gemountet wird (Vorgabe).
link_absolute	Symbolische Links bleiben unverändert.
map_identity	Auf dem Client werden die gleichen User-IDs wie auf dem Server verwendet (Vorgabe).
map_daemon	Client und Server haben keine übereinstimmenden User-IDs. Durch diese Option wird der nfsd angewiesen, eine Umsetztabelle für die User-IDs zu erstellen. Voraussetzung dafür ist jedoch die Aktivierung des Daemons ugidd.

Tabelle 12.12: *Zugriffsrechte für exportierte Verzeichnisse*

Die `exports`-Datei kann beispielsweise aussehen wie Datei 28.

```
#
# /etc/exports
#
/home            sonne(rw)   venus(rw)
/usr/X11         sonne(ro)   venus(ro)
/usr/lib/texmf   sonne(ro)   venus(rw)
/                erde(ro,root_squash)
/home/ftp        (ro)
# End of exports
```

Datei 28: `/etc/exports`

Die Datei `/etc/exports` wird von mountd und nfsd gelesen. Wird also eine Änderung daran vorgenommen, so müssen mountd und nfsd neu gestartet werden, damit diese Änderung berücksichtigt wird! Erreicht wird dies am einfachsten mit dem Befehl:

```
erde:~ #  rcnfsserver restart
```

DHCP

Das DHCP-Protokoll

Das so genannte „Dynamic Host Configuration Protocol“ dient dazu, Einstellungen in einem Netzwerk zentral von einem Server aus zu vergeben, statt diese dezentral an einzelnen Arbeitsplatzrechnern zu konfigurieren. Ein mit DHCP konfigurierter Client verfügt selbst nicht über statische Adressen, sondern konfiguriert sich voll und ganz selbstständig nach den Vorgaben des DHCP-Servers.

Dabei ist es möglich, jeden Client anhand der Hardware-Adresse seiner Netzwerkkarte zu identifizieren und ständig mit denselben Einstellungen zu versorgen, sowie Adressen aus einem dafür bestimmten Pool „dynamisch“ an jeden „interessierten“ Rechner zu vergeben. In diesem Fall wird sich der DHCP-Server bemühen, jedem Client bei jeder Anforderung (auch über längere Zeiträume hinweg) dieselbe Adresse zuzuweisen – dies funktioniert natürlich nicht, wenn es mehr Rechner im Netz als Adressen gibt.

Ein Systemadministrator kann somit gleich in zweierlei Hinsicht von DHCP profitieren. Einerseits ist es möglich, selbst umfangreiche Änderungen der Netzwerk-Adressen oder der Konfiguration komfortabel in der Konfigurationsdatei des DHCP-Servers zentral vorzunehmen, ohne dass eine Vielzahl von Clients einzeln konfiguriert werden müssen. Andererseits können vor allem neue Rechner sehr einfach ins Netzwerk integriert werden, indem sie aus dem Adress-Pool eine IP-Nummer zugewiesen bekommen. Auch für Laptops, die regelmäßig in verschiedenen Netzen betrieben werden, ist die Möglichkeit, von einem DHCP-Server jeweils passende Netzwerkeinstellungen zu beziehen, sicherlich interessant.

Neben IP-Adresse und Netzmaske werden der Rechner- und Domain-Name, der zu verwendende Gateway und Nameserver-Adressen dem Client mitgeteilt. Im Übrigen können auch etliche andere Parameter zentral konfiguriert werden, z. B. ein Timeserver, von dem die jeweils aktuelle Uhrzeit abrufbar ist oder ein Printserver. Im Folgenden möchten wir Ihnen nun einen kurzen Einblick in die Welt von DHCP geben. Wir möchten Ihnen anhand des DHCP-Servers dhcpd zeigen, wie einfach auch in Ihrem Netzwerk die gesamte Netzwerkkonfiguration zentral per DHCP erledigt werden kann.

DHCP-Softwarepakete

Bei SuSE Linux sind drei für DHCP relevante Pakete enthalten.

Einerseits gibt es den vom Internet Software Consortium herausgegebenen DHCP-Server `dhcpd`, der im Netzwerk die entsprechenden Einstellungen vergibt und verwaltet. Doch während bei SuSE Linux normalerweise nur `dhcpd` als Server in Frage kommt, stehen als DHCP-Clients zwei Alternativen zur Auswahl. Einerseits ist hier der ebenfalls von ISC herausgegebene dhclient zu nennen, andererseits der so genannte „DHCP Client Daemon" im Paket `dhcpcd`.

Der bei SuSE Linux standardmäßig installierte `dhcpcd` ist sehr einfach zu handhaben und wird beim Starten des Rechners automatisch gestartet, um nach einem DHCP-Server zu suchen. Er kommt ohne eine Konfigurationsdatei aus und sollte im Normalfall ohne weitere Konfiguration funktionieren.

Für komplexere Situationen kann man auf den ISC dhclient zurückgreifen, der sich über die Konfigurationsdatei `/etc/dhclient.conf` steuern lässt. Egal ob eine zusätzliche Domain in die Suchliste aufgenommen oder gar das Verhalten eines Microsoft DHCP-Clients emuliert werden soll – dem technisch versierten Anwender stehen unzählige Möglichkeiten zur Verfügung, das Verhalten des dhclient bis ins Detail seinen Bedürfnissen entsprechend anzupassen.

Der DHCP-Server dhcpd

Der *Dynamic Host Configuration Protocol Daemon* ist das Herz eines DHCP-Systems. Er „vermietet" Adressen und wacht über deren Nutzung, wie in der Konfigurationsdatei `/etc/dhcpd.conf` festgelegt. Über die dort definierten Parameter und Werte stehen dem Systemadministrator eine Vielzahl von Möglichkeiten zur Verfügung, das Verhalten des DHCP nach seinen Wünschen zu beeinflussen.

Ein Beispiel für eine einfache `/etc/dhcpd.conf`-Datei:

```
default-lease-time 600;         # 10 minutes
max-lease-time 7200;            # 2  hours

option domain-name "kosmos.all";
option domain-name-servers 192.168.1.1, 192.168.1.2;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option subnet-mask 255.255.255.0;
```

```
subnet 192.168.1.0 netmask 255.255.255.0
 {
  range 192.168.1.10 192.168.1.20;
  range 192.168.1.100 192.168.1.200;
 }
```

Datei 29: *Die Konfigurationsdatei* `/etc/dhcpd.conf`

Diese einfache Konfigurationsdatei reicht bereits aus, damit DHCP in Ihrem Netzwerk IP-Adressen zuweisen kann. Bitte achten Sie insbesondere auf die Strichpunkte am Ende jeder Zeile, ohne die dhcpd nicht starten wird!

Wie Sie sehen, lässt sich obige Beispieldatei in drei Blöcke unterteilen:

Im ersten Abschnitt wird definiert, wie viele Sekunden eine IP-Adresse standardmäßig an einen anfragenden Rechner „vermietet" wird, bevor sich dieser um eine Verlängerung bemühen sollte (`default-lease-time`). Auch wird hier angegeben, wie lange ein Rechner maximal eine vom DHCP-Server vergebene IP-Nummer behalten darf, ohne für diese eine Verlängerung zu beantragen (max-lease-time).

Im zweiten Block werden nun einige grundsätzliche Netzwerk-Parameter global festgesetzt:

- Mit `option domain-name` wird die Default-Domain Ihres Netzwerks definiert.
- Bei `option domain-name-servers` können bis zu drei DNS-Server angegeben werden, die zur Auflösung von IP-Adressen in Hostnamen (und umgekehrt) verwendet werden sollen. Idealerweise sollte auf Ihrem System bzw. innerhalb Ihres Netzwerks ein Nameserver bereits in Betrieb sein, der auch für dynamische Adressen jeweils einen Hostnamen und umgekehrt bereit hält. Mehr über die Einrichtung eines eigenen Nameservers erfahren Sie in Abschnitt 12 auf Seite 297.
- `option broadcast-address` legt fest, welche Broadcast-Adresse der anfragende Rechner verwenden soll.
- `option routers` definiert, wohin Datenpakete geschickt werden können, die (aufgrund der Adresse von Quell- und Zielhost sowie Subnetz-Maske) nicht im lokalen Netz zugestellt werden können. Gerade bei kleineren Netzen ist dieser Router auch meist der Übergang zum Internet.

- `option subnet-mask` gibt die an den Client zu übergebende Netzmaske an.

Unterhalb dieser allgemeinen Einstellungen wird nun noch ein Netzwerk samt Subnet Mask definiert. Abschließend muss noch ein Bereich gewählt werden, aus dem der DHCP-Daemon Adressen an anfragende Clients vergeben darf. Im Beispiel stehen alle Adressen zwischen `192.168.1.10` und `192.168.1.20` bzw. `192.168.1.100` und `192.168.1.200` zur Verfügung.

Nach diesen wenigen Zeilen sollten Sie bereits in der Lage sein, den DHCP-Daemon mit dem Kommando `rcdhcpd start` zu aktivieren, der sogleich zur Verfügung steht. Auch könnten Sie mit `rcdhcpd syntax-check` eine kurze, formale Überprüfung der Konfigurationsdatei vornehmen lassen. Sollte wider Erwarten ein Problem mit der Konfiguration auftreten und der Server mit einem Fehler abbrechen und nicht mit einem „done“ starten, finden Sie in der zentralen Systemprotokolldatei `/var/log/messages` meist ebenso Informationen dazu wie auf Konsole 10 (Ctrl + Alt + F10).

Rechner mit fester IP-Adresse

Nachdem wir es nun geschafft haben, den Server für die Vergabe von dynamischen Adressen zu konfigurieren, sollten wir uns die Vergabe *statischer* Adressen einmal genauer ansehen. Wie eingangs bereits erwähnt, kann mit DHCP auch an ein- und denselben Rechner bei jeder Anfrage eine ganz bestimmte, definierte Adresse vergeben werden.

Selbstverständlich haben solche expliziten Adresszuweisungen Vorrang vor solchen aus dem Pool der dynamischen Adressen. Im Gegensatz zu diesen verfallen die festen Adressinformationen in keinem Fall, wie es bei den dynamischen der Fall ist, wenn nicht mehr genügend freie Adressen zur Verfügung stehen und deshalb eine Neuverteilung erforderlich ist.

Zur Identifizierung eines mit einer *statischen* Adresse definierten Systems, bedient sich der DHCPD der so genannten Hardwareadresse. Dies ist eine weltweit i. d. R. einmalige, fest definierte Nummer aus sechs Oktettpaaren, über die jedes Netzwerkgerät verfügt, z. B. `00:00:45:12:EE:F4`.

Wird nun die Konfigurationsdatei aus Datei 29 auf Seite 318 um einen entsprechenden Eintrag wie in Datei 30 auf der nächsten Seite ergänzt, wird DHCPD unter allen Umständen dieselben Daten an den entsprechenden Rechner ausliefern.

```
host erde
 hardware ethernet 00:00:45:12:EE:F4;
 fixed-address 192.168.1.21;
```

Datei 30: *Ergänzungen zur Konfigurationsdatei*

Der Aufbau dieser Zeilen ist nahezu selbsterklärend:

Zuerst wird der DNS-Name des zu definierenden Rechners eingetragen (host *hostname*) und in der folgenden Zeile die MAC-Adresse definiert. Diese Adresse kann bei Linux-Rechnern mit dem Befehl `ifstatus` plus Netzwerkdevice (z. B. eth0) festgestellt werden. Gegebenenfalls müssen Sie zuvor die Karte aktivieren: `ifup eth0`. Sie erhalten dann eine Ausgabe wie: "link/ether 00:00:45:12:EE:F4".

In unserem Beispiel wird also dem Rechner, dessen Netzwerkkarte die MAC-Adresse `00:00:45:12:EE:F4` hat, die IP-Adresse `192.168.1.21` sowie der Rechnername `erde` zugewiesen.

Als Hardware-Typ wird heutzutage in aller Regel `ethernet` zum Einsatz kommen, wobei durchaus auch das vor allem bei IBM-Systemen häufig zu findende `token-ring` unterstützt wird.

Weitere Informationen

Wenn Sie an zusätzlichen Informationen interessiert sind, bietet sich z. B. die Seite des *Internet Software Consortium* an, auf der detaillierte Informationen zu DHCP verfügbar sind: `http://www.isc.org/products/DHCP/`.

Auch die neue Version 3 des Protokolls, die sich im Moment im Beta-Test befindet, wird dort dokumentiert. Im Übrigen stehen Ihnen selbstverständlich auch die Manpages zur Verfügung, dies sind insbesondere `man dhcpd`, `man dhcpd.conf`, `man dhcpd.leases` und `man dhcp-options`. Auf dem Markt sind bisweilen einige Bücher erschienen, die sich umfassend mit den Möglichkeiten des *Dynamic Host Name Configuration Protocol* auseinander setzen.

Übrigens, `dhcpd` kann sogar anfragenden Rechnern eine in der Konfigurationsdatei mit dem *filename*-Parameter definierte Datei anbieten, die einen bootbaren Betriebssystemkern enthält. Damit lassen sich Clients aufbauen, die über keine Festplatte verfügen und sowohl ihr Betriebssystem wie auch ihre Daten ausschließlich über das Netzwerk laden (*diskless clients*). Dies kann sowohl aus Kosten- als auch aus Sicherheitsgründen interessant sein.

Heterogene Netzwerke

Linux kann nicht nur mit anderen Linux-Rechnern, sondern auch mit Windows- und Macintosh-Rechnern sowie über Novell-Netzwerke kommunizieren. Dieses Kapitel zeigt Ihnen, worauf Sie dabei achten müssen und wie Sie entsprechende heterogene Netzwerke konfigurieren.

Samba 324
Netatalk 332
Netware-Emulation mit MARSNWE 339

Samba

Mit dem Programmpaket Samba kann ein beliebiger Unix-Rechner zu einem leistungsfähigen File- und Printserver für DOS-, Windows- und OS/2 Rechner ausgebaut werden. Das Samba-Projekt wird vom Samba Team betreut und wurde ursprünglich von dem Australier Andrew Tridgell entwickelt.

Samba ist inzwischen ein sehr umfassendes Produkt, so dass wir an dieser Stelle lediglich einen Einblick in seine Funktionalität liefern können. Jedoch kommt die Software mit umfassender digitaler Dokumentation. Diese besteht einerseits aus Handbuchseiten — zwecks Umfang rufen Sie bitte `apropos samba` auf der Kommandozeile auf — und andererseits aus Dokumenten und Beispielen, die Sie bei installiertem Samba auf Ihrem System unter `/usr/share/doc/packages/samba` finden. Dort finden Sie im Unterverzeichnis `examples` auch die kommentierte Beispielkonfiguration `smb.conf.SuSE`.

Samba benutzt das SMB-Protokoll (Server Message Block) der Firma Microsoft, das auf den NetBIOS Diensten aufgesetzt ist. Auf Drängen der Firma IBM gab die Firma Microsoft das Protokoll frei, sodass auch andere Software-Hersteller Anbindungen an ein Microsoft-Domain-Netz finden konnten. Samba setzt das SMB- auf das TCP/IP-Protokoll auf. Entsprechend muss auf allen Clients das Protokoll TCP/IP installiert sein. Wir empfehlen die ausschließliche Verwendung von TCP/IP auf den Clients.

NetBIOS

NetBIOS ist eine Softwareschnittstelle (API), die zur Rechnerkommunikation entworfen wurde. Dabei wird ein Namensdienst (engl. *name service*) bereitgestellt, der zur gegenseitigen Identifikation der Rechner dient. Für die Namensvergabe gibt es keine zentrale Instanz, die Rechte vergeben oder überprüfen könnte. Jeder Rechner am Netz kann beliebig Namen für sich reservieren, sofern diese noch nicht vergeben sind. Die NetBIOS-Schnittstelle kann auf unterschiedlichen Netzarchitekturen implementiert werden. Eine Implementation erfolgt relativ „dicht“ an der Netzwerkhardware und nennt sich NetBEUI. NetBEUI wird häufig als NetBIOS bezeichnet. Netzwerkprotokolle, mit denen NetBIOS implementiert wurde, sind IPX (NetBIOS über TCP/IP) von Novell und TCP/IP.

Die NetBIOS-Namen, die auch bei der Implementation von NetBIOS mittels TCP/IP vergeben werden, haben zunächst einmal nichts mit den in der Datei `/etc/hosts` oder per DNS vergebenen Namen zu tun, NetBIOS ist ein vollständig eigener Namensraum. Es empfiehlt sich jedoch zwecks vereinfachter Administration, zumindest für die Server NetBIOS-Namen zu vergeben, die ihrem DNS-Hostnamen entsprechen. Samba macht dies als Voreinstellung.

Clients

Alle gängigen Betriebssysteme wie DOS, Windows und OS/2 unterstützen das SMB-Protokoll. Auf den Rechnern muss das TCP/IP Protokoll installiert sein. Für die verschiedenen UNIX Versionen kann man ebenfalls Samba einsetzen.

SMB-Server stellen den Clients Plattenplatz in Form von Freigaben, so genannten „Shares“ zur Verfügung. Dabei umfasst ein Share ein Verzeichnis mit allen Unterverzeichnissen auf dem Server. Es wird unter einem eigenen Namen exportiert und kann von Clients unter diesem Namen angesprochen werden. Dabei kann der Sharename frei vergeben werden. Er muss nicht dem Namen des exportierten Verzeichnisses entsprechen. Ebenso wird einem exportierten Drucker ein Name zugeordnet, unter dem Clients darauf zugreifen können.

Installation und Konfiguration des Servers

Zunächst sollte das Paket `samba` installiert sein. Manuell startet man die Dienste mit `rcsmb start`; mit `rcsmb stop` kann man die Dienste beenden.

Die zentrale Konfigurationsdatei von Samba ist `/etc/samba/smb.conf`. Grundsätzlich ist die Datei in zwei Sektionen aufgeteilt. In der so genannten `[global]`-Section werden zentrale und übergreifende Einstellungen vorgenommen. Die zweite Sektion ist die `[share]`-Sektion. Hier werden die einzelnen Datei- und Drucker-Freigaben definiert. Dabei können Details der Freigaben unterschiedlich oder in der `[global]`-Sektion übergreifend gesetzt werden. Letzteres trägt zur Übersichtlichkeit der Konfigurationsdatei bei. Da im Betrieb häufig auf diese Datei zugegriffen wird, sorgt eine kurze und kommentarfreie Konfigurationsdatei für ein besseres Antwortverhalten des Samba-Servers.

Anschließend werden ausgewählte Paramter näher erläutert.

`global`-Section anhand der Beispielkonfiguration

Die folgenden Parameter der `global`-Section sind den Gegebenheiten Ihres Netzwerkes anzusassen, damit Ihr Samba-Server im Windows-Netz von anderen Systemen per SMB erreichbar ist.

- `workgroup = TUX-NET` Der Samba-Server wird mittels dieser Zeile einer Arbeitsgruppe zugeordnet. Zum Betrieb passen Sie `TUX-NET` an die bei Ihnen vorhandene Arbeitsgruppe an oder konfigurieren Ihren Clients auf den hier gewählten Wert. Ihr Samba-Server erscheint bei dieser

Konfiguration mit seinem DNS-Namen in der gewählten Arbeitsgruppe, insoweit der Name noch nicht vergeben ist.

Sollte der Name bereits vergeben sein, kann er mit `netbiosname= MEINNAME` abweichend vom DNS-Namen gesetzen werden. Details zu diesem Parameter sind per `man smb.conf` verfügbar.

- `os level = 2` Anhand dieses Parameters entscheidet Ihr Samba-Server, ob er versucht, LMB (engl. *Local Master Browser*) für seine Arbeitsgruppe zu werden. Der im Beispiel genutzte Wert ist bewusst niedrig gewählt, damit ein vorhandenes Windows-Netz nicht durch einen falsch konfigurierten Samba-Server gestört wird. Details zu diesem wichtigen Thema finden Sie in den Dateien `BROWSING.txt` und `BROWSING-Config.txt` im Unterverzeichnis `textdocs` der Paketdokumentation.

  Wird nicht bereits ein SMB-Server — z. B. Windows NT, 2000 Server — betrieben und soll der Samba-Server im lokalen Netz die Namen der verfügbaren Systeme vorhalten, so erhöhen Sie den `os level` auf einen höheren Wert (z. B. 65), um die Wahl zum LMB zu gewinnen.

  Bei der Änderung dieses Wertes sollten Sie besonders vorsichtig sein, da Sie den Betrieb eines vorhandenen Windows-Netzes stören können. Reden Sie mit Ihrem Administrator, testen Sie Änderungen zuerst in einem isolierten Netz oder zu unkritischen Zeiten.

- `wins support` und `wins server` Sie wollen den Samba-Server in ein vorhandenes Windows-Netz integrieren, in dem bereits ein WINS-Server betrieben wird: Dazu müssen Sie den Parameter `wins server` durch Entfernen des Semikolon aktivieren und die IP-Adresse auf Ihre Gegebenheiten anpassen.

  Ihre Windows-Systeme werden in getrennten Sub-Netzen betrieben, sollen sich gegenseitig sehen, in Ihrem Windows-Netz ist *kein* WINS-Server vorhanden und Ihr Samba-Server soll der WINS-Server werden: Aktivieren Sie dazu die Zeile mit `wins support = yes`. Achten Sie unbedingt darauf, dass Sie diesen Parameter ausschliesslich bei einem Samba-Server aktivieren. Zudem darf in dieser Konstellation `wins server` nicht aktiviert werden.

Freigaben

In den folgenden Beispielen werden einerseits das CD-ROM-Laufwerk und andererseits die Verzeichnise der Nutzer, `homes` für SMB-Clients freigegeben.

CD-ROM

```
;[cdrom]
;       comment = Linux CD-ROM
;       path = /media/cdrom
;       locking = no
```

***Datei 31:** CD-ROM-Freigabe*

Um die versehentliche Freigabe einer CD-ROM zu verhindern, sind alle erforderichen Zeilen dieser Freigabe deaktiviert.

- `[cdrom] und comment` Der Eintrag `[cdrom]` ist der den SMB-Clients sichtbare Freigabename. Mittels `comment` kann den Clients eine aussagekräftigere Bezeichnung der Freigabe mitgeteilt werden.
- `path = /media/cdrom` Mit `path` wird das Verzeichnis `/media/cdrom` exportiert.

Diese Art der Freigabe ist aufgrund einer bewusst restriktiv gewählten Voreinstellung lediglich für die auf dem System vorhandenen Nutzer verfügbar. Soll die Freigabe für jedermann bereitgestellt werden, ermöglicht man dies mit der zusätzlichen Zeile `guest ok = yes`. Aufgrund der sich daraus ergebenden Lesemöglichkeit für jedermann, sollte man mit dieser Einstellung sehr vorsichtig umgehen und sie allein auf ausgesuchte Freigaben anwenden. Für die Verwendung in der `[global]`-Section gilt besondere Vorsicht.

Eine besondere Stellung nimmt die sogenannte `[homes]`-Freigabe ein. Hat der Benutzer auf dem Linux-File-Server einen gültigen Account und ein eigenes Home-Verzeichnis, so kann sich sein Client bei gültiger Nutzerkennung und Passwort mit diesem verbinden.

```
[homes]
        comment = Home Directories
        valid users = %S
        browseable = no
        writeable = yes
        create mask = 0640
        directory mask = 0750
```

***Datei 32:** Freigabe homes*

- `[homes]` Insoweit keine ausdrückliche Freigabe mit dem Freigabenamen des sich verbindenden Nutzers existiert, wird aufgrund der `[homes]`-Freigabe dynamisch eine Freigabe erzeugt. Dabei ist der Freigabename identisch mit dem Nutzernamen.
- `valid users = %S` `%S` wird nach erfolfreichem Verbindungsaufbau durch dem konkreten Freigabenamen ersetzt. Da dies bei der `[homes]`-Freigabe immer mit dem Nutzernamen identisch ist, werden die zulässigen Nutzer auf den Eigentümer des Nutzerverzeichnisses beschränkt. Dies ist eine Möglichkeit, um den Zugriff allein dem Eigentümer zugestatten.
- `browseable = no` Durch diese Einstellung ist die `[homes]`-Freigabe nicht in der Liste der Freigaben sichtbar.
- `writeable = yes` Samba verbietet in der Voreinstellung den Schreibzugriff auf exportierte Freigaben, `read only = yes`. Soll also ein Verzeichnis als schreibbar freigegeben werden, muss man den Wert `writeable = yes` setzten. Bei Nutzerverzeichnisse ist dies in der Regel erwünscht.
- `create mask = 0640` Windows-Rechner kennen das Konzept der Unix-Zugriffsrechte nicht. Daher können sie bei der Erstellung von Dateien auch nicht angeben, mit welchen Zugriffsrechten dies zu geschehen hat.
  Der Parameter `create mask` legt fest, mit welchen Zugriffsrechten Dateien angelegt werden. Dieses gilt nur für schreibbare Shares. Konkret wird hier dem Eigentümer das Lesen und Schreiben und Mitgliegern der gleichen Gruppe das Lesen erlaubt. Bitte beachten Sie, dass `valid users = %S` selbst den lesenden Zugriff der Gruppenmitglieder verhindert.

Security Level

Das SMB-Protokoll kommt aus der DOS/Windows-Welt und berücksichtigt die Sicherheitsproblematik direkt. Jeder Zugang zu einem Share kann mit einem Passwort geschützt werden. SMB kennt drei verschiedene Möglichkeiten, dies zu bewerkstelligen:

- Share Level Security: Bei der Share Level Security wird einem Share ein Passwort fest zugeordnet. Jeder, der dieses Passwort kennt, hat Zugriff auf das Share.

- User Level Security: Diese Variante führt das Konzept des Benutzers in SMB ein. Jeder Benutzer muss sich bei einem Server mit einem Passwort anmelden. Nach der Authentifizierung kann der Server dann, abhängig vom Benutzernamen, Zugang zu den einzelnen, exportierten Shares gewähren.
- Server Level Security: Samba behauptet gegenüber den Clients, im User Level Mode zu arbeiten. Allerdings übergibt es alle Passwortanfragen an einen anderen User Level Mode Server, der die Authentifizierung übernimmt. Diese Einstellung erwartet einen weiteren Parameter (`password server =`).

Die Unterscheidung zwischen Share, User und Server Level Security gilt für den gesamten Server. Es ist nicht möglich, einzelne Shares per Share Level Security und andere per User Level Security zu exportieren.

Weitere Infos zu diesem Thema finden Sie in der Datei `textdocs/security_level.txt`.

Tipp

Für die einfache Administration des Samba-Servers gibt es noch das Programm swat. Es stellt ein einfaches Webinterface zur Verfügung, mit dem Sie bequem den Samba-Server konfigurieren können. Rufen Sie in einem Webbrowser `http://localhost:901` auf und loggen Sie sich als Benutzer root ein. Bitte beachten Sie, dass swat auch in den Dateien `/etc/inetd.conf` und `/etc/services` aktiviert ist. Weitere Informationen zu swat finden Sie in der Manual-Page von `swat` (`man swat`).

Tipp

Samba als Anmelde-Server

In Netzwerken, in denen sich überwiegend Windows-Clients befinden, ist es oft wünschenswert, dass sich die Benutzer nur mit gültigem Account und Passwort anmelden dürfen. Dies kann mit Hilfe eines Samba-Servers realisiert werden. In einem reinen Windows-Netzwerk übernimmt ein Windows-NT-Server diese Aufgabe, dieser ist als so genannter Primary Domain Controller (PDC) konfiguriert. Es müssen Einträge in die `[globals]`-Section der `smb.conf` vorgenommen werden wie in Beispiel 33 auf der nächsten Seite.

```
[global]
 workgroup = TUX-NET
 domain logons = yes
 domain master = yes%
```

Datei 33: *Global-Section in smb.conf*

Werden verschlüsselte Passwörter zur Verifizierung genutzt, muss der Samba Server damit umgehen können. Der Eintrag `encrypt passwords = yes` in der `[globals]`-Section ermöglicht dies. Außerdem müssen die Benutzeraccounts bzw. die Passwörter in eine Windows konforme Verschlüsselungsform gebracht werden. Das geschieht mit dem Befehl `smbpasswd -a name`. Da nach dem Windows NT Domänenkonzept auch die Rechner selbst einen Domänen-Account benötigen, wird dieser mit den folgenden Befehlen angelegt:

```
useradd -m rechnername
smbpasswd -a -m rechnername
```

Datei 34: *Anlegen eines Maschinenaccounts*

Bei dem Befehl `useradd` wurde ein Dollarzeichen, maskiert durch den Backslash hinzugefügt. Der Befehl `smbpasswd` fügt diesen bei der Verwendung des Parameters -m selbst hinzu.

In der kommentierten Beispielskonfiguration sind Einstellungen vorgesehen, die diese Arbeiten automatisieren.

```
add user script = /usr/sbin/useradd -g machines \
                  -c "NT Machine Account" -d
/dev/null -s /bin/false %m$
```

Datei 35: *Automatisiertes Anlegen eines Maschinenaccounts*

Installation der Clients

Zunächst sei erwähnt, dass die Clients den Samba-Server nur über TCP/IP erreichen können. NetBEUI oder NetBIOS über IPX sind mit Samba momentan nicht verwendbar. Da TCP/IP überall, sogar bei Novell und Microsoft, auf dem Vormarsch ist, ist es fraglich, ob sich dies jemals ändern wird.

Windows 9x/ME

Windows 9x/ME bringt die Unterstützung für TCP/IP bereits mit. Wie bei Windows for Workgroups wird sie jedoch in der Standardinstallation nicht mitinstalliert. Um TCP/IP nachzuinstallieren, wählt man im Netzwerk-Applet der Systemsteuerung 'Hinzufügen...' unter 'Protokolle' TCP/IP von Microsoft. Bitte achten Sie auf die korrekte Angabe Ihrer Netzwerkadresse und der Netzwerkmaske! Nach einem Neustart des Windows-Rechners können Sie den richtig konfigurierten Samba-Server in der Netzwerkumgebung wiederfinden (Doppelklick auf das entsprechende Icon auf dem Desktop).

Tipp

Um einen Drucker auf dem Samba-Server zu nutzen, sollte man den allgemeinen oder den Apple PostScript-Druckertreiber von der jeweiligen Windows-Version installieren; am besten verbindet man dann mit der Linux Drucker-Queue, die die automatische apsfilter-Erkennung beinhaltet.

Tipp

Optimierung

Eine Möglichkeit der Optimierung bietet `socket options`. Die Voreinstellung in der mitglieferten Beispielkonfiguration orientiert sich an einem lokalen Ethernet-Netzwerk. Weitere Details finden Sie in Manual-Page von `smb.conf` (`man smb.conf`) im Abschnitt `socket options` und zu Manual-Page von `socket(7)` (`man socket(7)`). Weitere Ansätze werden in `textdocs/Speed.txt` und `textdocs/Speed2.txt` beschrieben.

Die Standardkonfiguration in `/etc/samba/smb.conf` versucht weitestgehend sinnvolle Werte vorzuschlagen und verzichtet dabei auf alle Einstellungen, die den Voreinstellungen des Samba-Teams entsprechen. Dies ist jedoch insbesondere hinsichtlich der Netzwerkkonfiguration und des Arbeitsgruppennamens nur sehr schwer oder nicht möglich. In der kommentierten Beispielkonfiguration `examples/smb.conf.SuSE` finden Sie zahlreiche weiterführenden Hinweise, die bei der Anpassung an lokale Gegebenheiten hilfreich sind.

Tipp

Das Samba-Team liefert mit `textdocs/DIAGNOSIS.txt` eine Schritt-für-Schritt-Anleitung zum Überprüfen der Konfiguration.

Tipp

Netatalk

Mit dem Paket netatalk können Sie einen leistungsfähigen File- und Druckserver für Mac OS-Clients realisieren. Es ist möglich, von einem Macintosh aus auf Daten des Linux-Rechners zuzugreifen oder auf einem angeschlossenen Drucker zu drucken.

Netatalk ist eine Suite von Unix-Programmen, die auf dem im Kernel implementierten DDP (Datagram Delivery Protocol) aufsetzen und die AppleTalk-Protokoll-Familie (ADSP, ATP, ASP, RTMP, NBP, ZIP, AEP und PAP) implementieren.

AppleTalk ist im Prinzip ein Äquivalent zum wesentlich weiter verbreiteten TCP (Transmission Control Protocol). Viele auf TCP/IP aufsetzende Dienste, z. B. zur Auflösung von Hostnamen und Zeitsynchronisation, finden ihre Entsprechung unter AppleTalk. Beispielsweise wird anstelle von nslookup (DNS, Domain Name Service) der Befehl nbplkup (NBP, Name Binding Protocol) verwendet, und anstelle von ping (ICMP ECHO_REQUEST, Internet Control Message Protocol) der Befehl aecho (AEP, AppleTalk Echo Protocol).

Folgende drei Daemonen werden normalerweise auf dem Server gestartet:

- Der atalkd („AppleTalk-Netzwerk-Manager"), der quasi den Programmen ifconfig und routed entspricht;
- afpd (AppleTalk Filing Protocol daemon), der für Macintosh-Clients ein Interface zu Unix-Dateisystemen zur Verfügung stellt;
- papd (Printer Access Protocol daemon), der Drucker im (AppleTalk-) Netz bereitstellt.

Sie können ohne weiteres – und in heterogenen Netzwerkumgebungen ist dies sehr nützlich – Verzeichnisse auf dem Server nicht nur über Netatalk, sondern gleichzeitig über Samba (für Windows-Clients, siehe voriges Kapitel) und über NFS (siehe 12 auf Seite 312), exportieren. Datensicherung und die Verwaltung der Nutzerrechte können zentral auf dem Linux-Server erfolgen.

Beachten Sie bitte:

- Wegen einer Einschränkung der Macintosh-Clients dürfen die Passwörter der Benutzer auf dem Server maximal 8 Zeichen lang sein.
- Auf Unix-Dateien mit Namen länger als 31 Zeichen können Macintosh-Clients nicht zugreifen.
- Dateinamen dürfen keine Doppelpunkte (':') enthalten, weil diese unter Mac OS als Separator in Pfadnamen dienen.

Zu installieren ist das Paket netatalk.

Konfiguration des Fileservers

In der Standardkonfiguration ist Netatalk als Fileserver für die auf dem Linux-System eingetragenen Benutzer schon voll funktionsfähig. Um die weitergehenden Features zu nutzen, müssen Sie einige Einstellungen in den Konfigurationsdateien vornehmen. Diese befinden sich im Verzeichnis `/etc/atalk`.

Alle Konfigurationsdateien sind reine Textdateien. Text, der hinter einer Raute `'#'` steht, wird ignoriert („Kommentare"), leere Zeilen ebenso.

Netz konfigurieren – atalkd.conf

In `/etc/atalk/atalkd.conf` legt man fest, über welche Interfaces die Dienste angeboten werden. Meist ist dies `eth0`, und es genügt, wenn hier als einziger Wert

```
eth0
```

eingetragen ist (dies ist in der Beispieldatei der Fall). Hier tragen Sie weitere Interfaces ein, wenn Sie z. B. mehrere Netzwerkkarten gleichzeitig verwenden. Wird der Server gestartet, sucht er im Netzwerk nach bereits vorhandenen Zonen und Servern und verändert die entsprechende Zeile, indem er die konfigurierten AppleTalk-Netzwerk-Adressen einträgt. Sie finden dann eine Zeile wie

```
eth0 -phase 2 -net 0-65534 -addr 65280.57
```

am Ende der Datei. Sollten Sie komplexere Konfigurationen vornehmen wollen, finden Sie in der Konfigurationsdatei Beispiele. Dokumentation über weitere Optionen können Sie außerdem der Manual-Page zum afpd entnehmen.

Fileserver definieren – afpd.conf

In der Datei `afpd.conf` wird festgelegt, wie Ihr Fileserver auf Mac-OS-Rechnern in der 'Auswahl' erscheint. Wie die anderen Konfigurationsdateien enthält auch diese ausführliche Kommentare, die die vielfältigen Optionen erklären.

Ändern Sie hier nichts, wird einfach der Default-Server gestartet und in der 'Auswahl' mit dem Hostnamen angezeigt. Sie müssen also hier nicht unbedingt etwas eintragen, allerdings ist es auch möglich, Fileserver mit verschiedenen Namen und Optionen zu definieren, um z. B. einen speziellen „Guest Server" anzubieten, auf dem man als „Gast" Dateien ablegen kann:

```
"Guest server" -uamlist uams_guest.so
```

Oder Sie können einen Server definieren, der keinen Gastzugang erlaubt, sondern nur für Benutzer zugänglich ist, die auf dem Linux-System existieren:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so
```

Dieses Verhalten wird gesteuert durch die Option `uamlist` gefolgt von einer durch Kommata getrennten Liste der zu verwendenden Authentifizierungsmodule. Default ist, dass alle Verfahren aktiv sind.

Ein AppleShare-Server stellt seine Dienste standardmäßig nicht nur über AppleTalk, sondern auch („encapsulated") über TCP/IP zur Verfügung. Der Default-Port ist 548. Für zusätzliche AppleShare-Server (auf dem gleichen Rechner) müssen Sie, wenn diese ebenfalls auch über TCP laufen sollen, dedizierte Ports zuweisen. Die Bereitstellung des Dienstes über TCP/IP ermöglicht den Zugriff auf den Server auch über nicht AppleTalk-Netze wie zum Beispiel das Internet.

Die Syntax wäre dann z. B.:

```
"Font server" -uamlist uams_clrtxt.so,uams_dhx.so -port 12000
```

Der AppleShare-Server erscheint hier im Netz mit dem Namen „Font Server", erlaubt keinen Zugriff für Gäste und ist auf den Port 12 000 eingestellt. Damit ist er auch über TCP/IP-Router hinweg erreichbar.

Welche (auf dem Server liegenden) Verzeichnisse der jeweilige AppleShare-Server dann als Netz-„Volumes" bereitstellt, wird in der Datei `AppleVolumes.default` definiert (die weiter unten näher erläutert wird). Mit der `-defaultvol` Option können Sie für einen einzelnen AppleShare-Server auch eine andere Datei festlegen, in der abweichende Vorgaben gemacht werden, z. B. (in einer Zeile):

```
"Guest server" -uamlist uams_guest.so -defaultvol
/etc/atalk/AppleVolumes.guest
```

Weitere Optionen sind in der Datei `afpd.conf` selbst erklärt.

Verzeichnisse und Zugriffsrechte – AppleVolumes.default

Hier legen Sie Verzeichnisse fest, die exportiert werden sollen. Die Zugriffsrechte werden dabei durch die unter Unix üblichen Benutzer- und Gruppen-Rechte festgelegt.

Dies wird in der Datei `AppleVolumes.default` eingerichtet.

Hinweis

Hier hat sich die Syntax teilweise geändert. Bitte berücksichtigen Sie dies, wenn Sie von einer älteren Version updaten; z. B. heißt es statt `access=` jetzt `allow:` (ein charakteristisches Symptom wäre, wenn Sie auf den Mac-Clients unter AppleTalk statt der Laufwerksbezeichnung deren Optionen angezeigt bekommen.) Da bei einem Update die neuen Dateien mit der Endung `.rpmnew` angelegt werden, kann es sein, dass Ihre alten Einstellungen unter Umständen wegen der geänderten Syntax nicht mehr funktionieren.

Wir empfehlen Ihnen, ein Backup von Ihren Konfigurationsdateien zu machen, aus diesen Ihre alten Einstellungen in die neuen Dateien zu übernehmen und diese dann umzubenennen. So profitieren Sie auch von den aktuellen ausführlichen Kommentaren, die zur Erklärung der diversen Optionen in den Konfigurationsdateien enthalten sind.

Hinweis

Neben `AppleVolumes.default` können zusätzliche Dateien angelegt werden, z. B. `AppleVolumes.guest`, die von bestimmten Servern benutzt werden (indem in der Datei `afpd.conf` die `-defaultvol`-Option benutzt wird – siehe voriger Abschnitt).

Die Syntax ist denkbar einfach:

```
/usr/local/psfonts "PostScript Fonts"
```

bedeutet, dass das in dem Rootverzeichnis liegende Linux-Verzeichnis `/usr/local/psfonts` als AppleShare-Volume mit dem Namen „PostScript Fonts“ freigegeben wird.

Optionen werden, durch Leerzeichen getrennt, an die Zeile angehängt. Eine sehr nützliche Option ist die Zugriffsbeschränkung:

```
/usr/local/psfonts "PostScript Fonts" allow:User1,@gruppe0
```

was den Zugriff auf das Volume „PostScript Fonts“ auf den Benutzer „User1“ und alle Mitglieder der Gruppe „gruppe0“ beschränkt. Diese müssen natürlich dem Server bekannt sein. Entsprechend können Sie mit `deny:User2` auch explizit Nutzer ausschließen.

Bitte berücksichtigen Sie, dass diese Einschränkungen für den Zugriff über AppleTalk gelten und nichts mit den Rechten zu tun haben, die der User hat, wenn er sich auf dem Server selber einloggen kann.

Netatalk legt zur Abbildung der Mac-OS-typischen Ressource-Fork von Dateien im Linux-Dateisystem `.AppleDouble`-Verzeichnisse an. Mit der Option `noadouble` können Sie bestimmen, dass diese Verzeichnisse erst dann angelegt werden, wenn sie tatsächlich benötigt werden. Syntax:

```
/usr/local/guests "Guests" options:noadouble
```

Weitere Optionen und Möglichkeiten entnehmen Sie bitte den Erklärungen in der Datei selbst.

Übrigens: In dieser Konfigurationsdatei finden Sie ebenfalls eine kleine unschuldige Tilde ('~'). Diese Tilde steht für das Homeverzeichnis eines jeden Benutzers auf dem Server. Dadurch kann jedem Benutzer automatisch sein Homeverzeichnis bereitgestellt werden, ohne dass jedes einzelne hier explizit angegeben werden müsste. Die installierte Beispieldatei enthält bereits eine Tilde, weshalb Netatalk standardmäßig die Homeverzeichnisse bereitstellt, wenn Sie an dieser Datei nichts ändern.

Der afpd sucht außerdem im Homeverzeichnis eines angemeldeten Benutzers nach einer Datei `Applevolumes` oder `.Applevolumes`. Einträge in dieser Datei ergänzen die Einträge in den Serverdateien `AppleVolumes.system` und `AppleVolumes.default`, um weitere individuelle type/creator-Zuordnungen zu ermöglichen und auf Dateisysteme zuzugreifen. Diese Einträge sind Ergänzungen und ermöglichen keine Zugriffe, die nicht von Serverseite für diesen Benutzer erlaubt sind.

Die Datei `netatalk.pamd` dient der Authentifizierung über PAM (Pluggable Authentication Modules), was in unserem Rahmen hier ohne Bedeutung ist.

Dateizuordnungen – `AppleVolumes.system`

In der Datei `AppleVolumes.System` legen Sie fest, welche (Mac-OS-typischen) Type- und Creator-Zuordnungen zu bestimmten Dateiendungen erfolgen soll. Eine ganze Reihe von Standardwerten sind schon vorgegeben. Wenn eine Datei mit einem generischen weißen Icon angezeigt wird, ist in diesem Fall noch kein Eintrag vorhanden. Sollten Sie Probleme haben, eine Textdatei eines anderen Systems unter Mac OS korrekt öffnen zu können, bzw. das umgekehrte Problem, kontrollieren Sie dort die Einträge.

Konfiguration des Druckservers

Über die Datei papd.conf konfigurierbar wird ein Laserwriter-Dienst zur Verfügung gestellt. Der Drucker muss lokal schon mit dem lpd funktionieren. Wenn Sie mit dem Kommando lpr datei.txt lokal drucken können, ist der erste Schritt erfolgreich getan.

Sie müssen in papd.conf nichts eingeben, wenn unter Linux ein lokaler Drucker eingerichtet ist, da ohne weitere Angaben Druckaufträge einfach an den Druck-Daemon lpd weitergegeben werden. Der Drucker meldet sich im AppleTalk-Netz als Laserwriter. Sie können aber auch bestimmte Drucker wie folgt eintragen:

```
Drucker_Empfang:pr=lp:pd=/etc/atalk/kyocera.ppd
```

Dies lässt den Drucker mit dem Namen Drucker_Empfang in der Auswahl erscheinen. Die entsprechende Druckerbeschreibungsdatei gibt es gewöhnlich beim Hersteller. Ansonsten nehmen Sie einfach die Datei Laserwriter aus dem Ordner 'Systemerweiterungen'; allerdings können Sie dann meist nicht alle Features benutzen.

Starten des Servers

Der Server wird per „Init-Skript" beim Systemstart gestartet oder per Hand mit: rcatalk start. Das Init-Skript befindet sich in /etc/init.d/atalk. Den Start erledigt das Startskript im Hintergrund; es dauert ca. eine Minute, bis die AppleTalk-Interfaces konfiguriert und erreichbar sind. Sie können mit einer Statusabfrage sehen, ob es soweit ist (erkennbar daran, dass dreimal OK ausgegeben wird):

```
erde:~ #  rcatalk status
```

"Checking for service atalk:OKOKOK"

Gehen Sie nun an einen Mac, der unter Mac OS läuft. Kontrollieren Sie, dass AppleTalk aktiviert ist, wählen Sie 'Filesharing', doppelklicken Sie 'Appleshare'; in dem Fenster sollten Sie nun den Namen Ihres Servers sehen. Doppelklicken Sie ihn und melden sie sich an. Wählen Sie das Laufwerk und – voilà – hier ist Ihr Netzlaufwerk unter Mac OS.

Mit Servern, die nur über TCP und nicht über DDP laufen, können Sie sich verbinden, indem Sie in der 'Auswahl' auf 'Server IP-Adresse' klicken und die entsprechende IP-Adresse, gegebenenfalls gefolgt von einem Doppelpunkt und der Portnummer, eingeben.

Weiterführende Informationen

Um alle Möglichkeiten, die das Paket `netatalk` bietet, voll auszuschöpfen, empfiehlt es sich, in den entsprechenden Manual-Pages zu stöbern. Diese finden Sie mit dem Befehl: `rpm -qd netatalk` Noch ein Hinweis: Die Datei `/etc/atalk/netatalk.conf` wird in unserer Version von netatalk nicht verwendet, Sie können sie einfach ignorieren. Hilfreiche URLs:

- `http://netatalk.sourceforge.net/`
- `http://www.umich.edu/~rsug/netatalk/`
- `http://www.anders.com/projects/netatalk/`
- `http://cgi.zettabyte.net/fom-serve/netatalk/cache/1.html`

Und wie sieht es eigentlich „andersherum“ aus? Kann ich unter Linux ein AppleShare-Laufwerk erreichen? Die ehrlichste Antwort ist: Besser nicht, da das entsprechende Paket, sich in einem Prä-Alpha-Stadium befindet. Tapfere Experimentatoren finden es unter: `http://www.panix.com/~dfoster/afpfs/`

Netware-Emulation mit MARSNWE

Der Netware-Emulator MARSNWE kann einen Novell-Netware 2.2 bzw. 3.11 Server für Datei- und Druckdienste relativ leicht ersetzen und kann dabei auch als IPX-Router verwendet werden. Die Funktionalität neuerer Netware Versionen, wie z. B. NDS (engl. *Netware Directoy Services*) kann er allerdings nicht bieten. Arbeitsstationen, die mit DOS oder Windows laufen und bereits für den Zugriff auf einen Netware 2.2/3.11/3.12-Server konfiguriert sind, können mit minimalen Änderungen den Linux-Server mit dem Netware-Emulator MARSNWE als Server nutzen. Die Administration erledigt man am besten unter Linux, da die Novell-Programme zur Systemadministration nur bedingt verwendbar sind und dabei auch Lizenzen zu beachten sind.

Netware Emulator MARSNWE starten

Der MARSNWE auf SuSE Linux kann sofort nach der Installation gestartet werden, da er bereits soweit vorkonfiguriert ist, dass man ihn sofort testen kann. Die erforderliche IPX-Unterstützung seitens des Kernels ist als ladbares Kernelmodul vorhanden und wird vom Startskript bei Bedarf automatisch geladen. Das Aufsetzen des IPX-Interfaces wird vom MARSNWE automatisch durchgeführt. Netznummer und zu verwendendes Protokoll werden dabei der ausführlich kommentierten Konfigurationsdatei `/etc/nwserv.conf` entnommen. Gestartet wird der MARSNWE mit dem Kommando `rcnwe start`. Meldet er dabei am rechten Bildschirmrand in grün `done`, wurde er erfolgreich gestartet.

Ob der Netware-Emulator läuft, überprüft man mit `rcnwe status`, und beendet wird er mit `rcnwe stop`.

Die Konfigurationsdatei /etc/nwserv.conf

Die Konfigurationsoptionen sind zu „Sections" zusammengefasst, die einfach durchnummeriert werden. Jede Konfigurationszeile beginnt dabei immer mit der Nummer der jeweiligen Section. Interessant sind lediglich die Sections 1 bis 22, wobei aber nicht alle Nummern verwendet werden. Im Normalfall kommt man mit folgenden Sections für die Konfiguration aus:

1 Netware Volumes

2 Servername

4 IPX-Netzwerk

13 Benutzernamen

21 Drucker

Nach Änderungen an der Konfiguration, muss MARSNWE mit dem Befehl `rcnwe restart` neu gestartet werden.

Die Konfigurations-Optionen im Detail:

Volumes (Section 1):

```
1    SYS    /usr/local/nwe/SYS/    kt     711 600
```

Hier werden die zu exportierenden Volumes definiert. Jede Zeile beginnt mit der Nummer der Section (hier 1), danach folgt der Volume-Name und dann der Pfad des Verzeichnisses auf dem Server. Zusätzlich können noch diverse Optionen angegeben werden, die durch einzelne Buchstaben dargestellt sind, sowie jeweils eine UMASK für das Erzeugen von Verzeichnissen und eine für Dateien. Wird keine UMASK angegeben, wird der Standardwert aus Section 9 verwendet. Das Volume für SYS ist bereits eingetragen. Um Probleme mit Groß- und Kleinschreibung bei Dateinamen zu vermeiden, empfiehlt sich die Verwendung der Option `k`, denn dann werden alle Dateinamen in Kleinschreibung konvertiert.

Servername (Section 2):

```
2    MARS
```

Diese Angabe ist Optional, standardmäßig wird der Hostname verwendet.

Interne Netznummer (Section 3):

```
3    auto
```

Die interne Netznummer wird aus der MAC-Adresse der Netzwerkkarte generiert, wenn hier `auto` angegeben ist. Normalerweise behält man diese Einstellung bei.

IPX-Konfiguration (Section 4):

```
4    0x0     *       AUTO           1
4    0x22    eth0    ethernet_ii    1
```

Hier gibt man die Netware-Netznummer an und auf welche Netzwerk-Schnittstelle es mit welchem Protokoll gebunden werden soll. Das erste Beispiel setzt alles automatisch auf, während das zweite die Netznummer `0x22` auf die Netzwerkkarte `eth0` mit dem Frametyp `Ethernet-II` bindet. Hat man mehrere Netzwerkkarten und trägt diese alle mit unterschiedlichen Netznummern ein, so wird IPX dazwischen geroutet.

Create Mode (Section 9):

```
9    0751    0640
```

Gibt die Standardrechte an, mit denen Verzeichnisse und Dateien angelegt werden.

GID und UID mit minimalen Rechten (Section 10, 11):

```
10   65534
11   65534
```

Gruppen- und Benutzer-ID für nicht angemeldete Benutzer. Hier `nogroup` und `nobody`.

Supervisor Login (Section 12):

```
12   SUPERVISOR      root
```

Der Supervisor wird auf den Benutzer root abgebildet.

Benutzer Logins (Section 13):

```
13   LINUX           linux
```

Die Zuordnung der Netware-Benutzer zu den Linux-Usern wird hier festgelegt. Optional kann ein festes Passwort mit eingetragen werden.

Automatische Benutzer-Abbildung (Section 15):

```
15   0       top-secret
```

Gibt man hier statt der `0` eine `1` an, werden die Linux Logins automatisch als Netware Logins zur Verfügung gestellt, das Passwort ist in diesem Fall „top-secret“.

Drucker-Queues (Section 21):

```
21   LP      -       lpr -
```

Der erste Parameter LP ist der Name des Netware-Druckers, als zweites kann man den Namen des Spool-Verzeichnisses angeben und als drittes das Druckkommando.

Print-Server (Section 22):

```
22   PS_NWE  LP_PS   1
```

Drucker die über pserver aus dem Paket ncpfs angesprochen werden, können hier definiert werden.

Zugriff auf Netware-Server und deren Administration

Das Paket ncpfs ist eine Sammlung kleiner Programme, mit denen man einen Netware 2.2/3.11 Server von Linux aus administrieren, Netware-Volumes mounten oder Drucker verwalten kann. Will man auf neuere Netware-Server ab Version 4 zugreifen, muss auf diesen die Bindery-Emulation und IPX aktiviert sein.

Folgende Programme stehen dafür zur Verfügung, deren Funktion man den Manpages dazu entnehmen kann:

nwmsg	ncopy	ncpmount	ncpumount
nprint	nsend	nwauth	nwbocreate
nwbols	nwboprops	nwborm	nwbpadd
nwbpcreate	nwbprm	nwbpset	nwbpvalues
nwdir	nwdpvalues	nwfsctrl	nwfsinfo
nwfstime	nwgrant	nwpasswd	nwpurge
nwrevoke	nwrights	nwsfind	nwtrustee
nwtrustee2	nwuserlist	nwvolinfo	pqlist
pqrm	pqstat	pserver	slist

Wichtig ist z. B. ncpmount, mit dem man Volumes von einem Netware-Server unter Linux mounten kann und ncpumount um es wieder zu unmounten.

Außerdem enthält das Paket ncpfs Tools zur Konfiguration des IPX-Protokolls und IPX-Routing:

```
ipx_cmd
ipx_configure
ipx_interface
ipx_internal_net
ipx_route
```

Mit `ipx_configure` oder `ipx_interface` kann man die IPX-Konfiguration der Netzwerkkarte vornehmen. Hat man MARSNWE laufen macht dieser das aber bereits automatisch.

IPX-Router mit ipxrip

Ein weiteres Paket, um Linux in einen IPX-Router zu verwandeln ist Paket `ipxrip`. In der Regel wird man es aber nicht benötigen, da man mit MARSNWE oder den Tools aus Paket `ncpfs` ebenfalls einen IPX-Router konfigurieren kann.

Internet

Zum Thema Internet ließe sich vieles schreiben, doch im Rahmen dieses Buches beschränken wir uns auf zwei Themen: die manuelle Konfiguration eines ADSL-Zuganges, falls es bei der Einrichtung mit YaST2 Probleme geben sollte, und die Konfiguration des Proxies Squid.

Konfiguration eines ADSL / T-DSL Anschlusses 346
Proxy-Server: Squid 347

Konfiguration eines ADSL / T-DSL Anschlusses

Standardkonfiguration

Momentan werden von SuSE Linux DSL-Zugänge unterstützt, die mit dem Point-to-Point-over-Ethernet-Protokoll (PPPoE) arbeiten. Dieses Protokoll wird von allen großen Anbietern benutzt. Sollten Sie sich nicht sicher sein, welches Protokoll Ihr Provider verwendet, gibt dieser sicherlich gerne Auskunft.

1. Die Pakete `ppp` und `smpppd` müssen installiert werden. Verwenden Sie dazu am besten YaST2.

2. Konfigurieren Sie ihre Netzwerkkarte mit YaST2. Verwenden Sie nicht `dhcp`, sondern vergeben Sie eine statische IP Adresse, zum Beispiel `192.168.2.22`.

3. Die Parameter, die Sie mit dem YaST2 T/ADSL-Modul bearbeiten, wer- den in der Datei `/etc/sysconfig/network/providers/dsl-provider0` abgespeichert. Zusätzlich gibt es noch Konfigurationsdateien für den SuSE Meta-PPP-Daemon und seine Frontends kinternet und cinternet. Bitte beachten Sie dazu Manual-Page von `smpppd` (`man smpppd`).

4. Starten Sie das Netzwerk ggf. mit dem Befehl `rcnetwork start`.

5. Mit den Befehlen `cinternet -start` und `cinternet -stop` können Sie auf einem System ohne graphischer Oberfläche eine Verbindung herstellen bzw. abbrechen. Auf einer graphischen Benutzer-Oberfläche können Sie dazu kinternet benutzen, das automatisch gestartet wurde, falls Sie DSL mit YaST2 eingerichtet haben. Klicken Sie auf das Zahnrad-Icon in der Buttonleiste. Wählen Sie 'Kommunikation/Internet' → 'Internet Tools' → 'kinternet'. Nun erscheint in der Buttonleiste das Steckersymbol. Ein Klick darauf startet die Verbindung und ein zweiter Klick beendet sie wieder.

DSL Verbindung per Dial-on-Demand

Dial-on-Demand bedeutet, dass die Verbindung automatisch aufgebaut wird, sobald ein User auf das Internet zugreift, z. B. indem er eine Webseite mit einem Browser anwählt oder E-Mails verschickt. Nach einer bestimmten Zeit (Idletime), in der keine Daten gesendet oder empfangen werden, wird die Verbindung wieder getrennt. Da die Einwahl mit PPPoE, dem Protokoll für

ADSL, sehr schnell geht, entsteht fast der Eindruck, als hätte man eine Standleitung in das Internet.

Dies ist aber nur sinnvoll, wenn Sie eine so genannte Flatrate besitzen. Wird Ihr Zugang zeitabhängig abgerechnet, müssen Sie darauf achten, dass kein periodischer Prozess, z. B. ein cronjob, immer wieder eine Verbindung aufbaut. Das könnte sehr teuer werden.

Obwohl mit einer DSL-Flatrate auch eine permanente Einwahl möglich wäre, sprechen doch einige Punkte für eine Verbindung, die nur kurz und nach Bedarf besteht:

- Die meisten Provider trennen die Verbindung nach einer gewissen Zeit.
- Eine permanente Verbindung kann als Ressourcenverschwendung betrachtet werden (z. B. IP-Adressen).
- Vor allem ist es ein enormes Sicherheitsrisiko permanent online zu sein, da ein Angreifer das System auf Schwachstellen absuchen kann. Ein System, das nur bei Bedarf im Internet erreichbar ist und immer wieder eine andere IP-Adresse hat, ist viel schwieriger zu attackieren.

Dial-on-Demand können Sie mit YaST2 aktivieren (siehe auch das Benutzer-Handbuch) oder Sie richten es manuell ein. Setzen Sie in der Datei `/etc/sysconfig/network/providers/dsl-provider0` den Parameter `DEMAND=` auf „yes“ und definieren Sie eine Idletime mit der Variable: `IDLETIME="60"`. Damit wird eine unbenutzte Verbindung nach 60 Sekunden beendet.

Zur Einrichtung eines DSL-Gateways für private Netzwerke empfehlen wir folgenden Artikel in unserer Supportdatenbank: `http://sdb.suse.de/de/sdb/html/masq80.html`

Proxy-Server: Squid

Squid ist der am weitesten verbreitete Proxy-Cache für Linux/UNIX-Plattformen. Wir werden beschreiben, wie er zu konfigurieren ist, welche Systemanforderungen bestehen, wie das eigene System konfiguriert sein muss, um transparentes Proxying durchzuführen, wie man Statistiken über den Nutzen des Cache mithilfe von Programmen wie Calamaris und cachemgr erhält oder wie man Web-Inhalte mit squidgrd filtert.

Was ist ein Proxy-Cache?

Squid fungiert als Proxy-Cache. Es verhält sich wie ein Makler, der Anfragen von Clients erhält (in diesem Fall Web-Browser) und an den zuständigen Server-Provider weiterleitet. Wenn die angeforderten Objekte beim Vermittler ankommen, behält er eine Kopie davon in einem Festplatten-Cache.

Der Vorteil zeigt sich, wenn mehrere Clients dasselbe Objekt anfordern: Sie können nun direkt aus dem Festplatten-Cache bedient werden, also wesentlich schneller als aus dem Internet. Dies spart gleichzeitig eine Menge Systembandbreite.

Tipp

Squid bietet ein großes Spektrum an Features, z. B. die Festlegung von Hierarchien für die Proxy-Server zum Verteilen der Systemlast, Aufstellen fester Zugriffsregeln an alle Clients, die auf den Proxy zugreifen wollen, Erteilen oder Verweigern von Zugriffsrechten auf bestimmte Webseiten mit Hilfe anderer Applikationen oder die Ausgabe von Statistiken der meistbesuchten Webseiten, wie z. B. das Surfverhalten der Benutzer u. v. m.

Tipp

Squid ist kein generischer Proxy. Normalerweise vermittelt er nur zwischen HTTP-Verbindungen. Außerdem unterstützt er die Protokolle FTP, Gopher, SSL und WAIS, jedoch keine anderen Internet-Protokolle wie Real Audio, News oder Videokonferenzen. Squid greift auf das UDP-Protokoll nur zur Unterstützung der Kommunikation zwischen verschiedenen Caches zurück. Aus diesem Grund werden auch andere Multimedia-Programme nicht unterstützt.

Informationen zu Proxy-Cache

Squid und Sicherheit

Man kann Squid zusammen mit einer Firewall verwenden, um interne Netzwerke durch den Einsatz von Proxy-Cache nach außen zu schützen. Die Firewall verweigert mit Ausnahme von Squid alle externen Dienste, alle WWW-Verbindungen müssen durch den Proxy aufgebaut werden.

Im Falle einer Firewall-Konfiguration mit einem DMZ würden wir dort unseren Proxy setzen. In diesem Fall ist es wichtig, dass alle Rechner im DMZ ihre Protokolldateien an Rechner innerhalb des gesicherten Netzwerks senden.

Ein Möglichkeit der Implementierung dieser Features mit Hilfe eines so genannten „transparenten“ Proxy wird in Abschnitt *Transparente Proxy-Konfiguration* auf Seite 359 behandelt.

Mehrere Caches

Man kann mehrere Caches so konfigurieren, dass Objekte zwischen ihnen ausgetauscht werden können, um die Systemlast zu reduzieren und die Möglichkeit zu steigern, ein bereits im lokalen Netzwerk vorhandenes Objekt zu finden. Möglich sind auch Cache-Hierarchien, so dass ein Cache in der Lage ist, Objektanfragen an Caches der gleichen Hierarchie weiterzuleiten oder einen übergeordneten Cache zu veranlassen, die Objekte von einem anderen Cache im lokalen Netzwerk oder direkt aus der Quelle herunterzuladen.

Die Wahl der richtigen Topologie für die Cache-Hierarchie ist sehr wichtig, da Netzwerkverkehr insgesamt nicht erhöht werden soll. In einem großen Netzwerk z. B. ist es möglich, für jedes Subnetz einen Proxy-Server zu konfigurieren und diesen dann mit einem übergeordneten Proxy zu verbinden, der wiederum an den Proxy-Cache vom ISP angeschlossen wird.

Die gesamte Kommunikation wird vom ICP (engl. *Internet Cache Protocol*) gesteuert, das auf dem UDP-Protokoll aufgesetzt ist. Der Datenaustausch zwischen Caches geschieht mittels HTTP (engl. *Hyper Text Transmission Protocol*) basierend auf TCP. Allerdings sollten für solche Verbindungen schnellere und einfachere Protokolle verwendet werden, die innerhalb von maximal einer oder zwei Sekunden auf eingehende Anfragen reagieren können.

Um den besten Server für die gewünschten Objekte zu finden, schickt ein Cache an alle Proxies der gleichen Hierarchie eine ICP-Anfrage. Die Proxies werden mittels ICP-Antworten mit dem Code „HIT“ auf die Anfragen reagieren, falls das Objekt gefunden wurde oder, falls nicht, mit dem Code „MISS“. Im Falle mehrerer HIT-Antworten wird der Proxy-Server einen Server für das Herunterladen bestimmen. Diese Entscheidung wird unter anderem dadurch bestimmt, welcher Cache die schnellste Antwort sendet oder welcher näher ist. Bei einer nicht zufrieden stellenden Antwort gesendet wurde, wird die Anfrage an den übergeordneten Cache geschickt.

Tipp

Zur Vermeidung von mehrfacher Speicherung von Objekten in verschiedenen Caches unseres Netzwerks werden andere ICP-Protokolle verwendet, wie z. B. CARP (engl. *Cache Array Routing Protocol*) oder HTCP (engl. *Hyper-Text Cache Protocol*).

Je mehr Objekte sich im Netzwerk befinden, desto leichter wird es, das Gesuchte zu finden.

Tipp

Zwischenspeichern von Internetobjekten

Nicht alle im Netzwerk verfügbaren Objekte sind statisch. Es existieren viele dynamisch generierte CGI-Seiten, Zugriffszähler oder verschlüsselte SSL-Dokumente für eine höhere Sicherheit. Aus diesem Grund werden solche Objekte nicht im Cache gehalten: Bei jedem neuen Zugriff hat sich das Objekt bereits wieder verändert.

Für alle anderen im Cache befindlichen Objekte stellt sich jedoch die Frage, wie lange sie dort bleiben sollen. Für diese Entscheidung werden alle Objekte im Cache drei verschiedenen Stadien zugeordnet:

Durch Header wie `Last modified` („zuletzt geändert") oder `Expires` („läuft ab") und dem entsprechenden Datum informieren sich Web- und Proxy-Server über den Status eines Objekts. Es werden auch andere Header verwendet, die z. B. anzeigen, dass ein Objekt nicht zwischengespeichert werden muss.

Objekte im Cache werden normalerweise aufgrund fehlenden Speichers ersetzt, und zwar durch Algorithmen wie LRU (engl. *Last Recently Used*), die zum Ersetzen von Cache-Objekten entwickelt wurden. Das Prinzip besteht im Wesentlichen darin, zuerst die am seltensten gewünschten Objekte zu ersetzen.

Systemanforderungen

Zuerst sollte die maximale Systemlast bestimmt werden. Es ist wichtig, den Systemspitzen besondere Aufmerksamkeit zu schenken, da diese mehr als viermal so hoch wie der Tagesdurchschnitt sein können. Im Zweifelsfall ist es besser, die Systemanforderungen zu überschätzen, vorausgesetzt, dass ein am Limit arbeitender Squid zu einem ernsthaften Qualitätsverlust des Dienstes führen kann.

Geordnet nach Wichtigkeit werden in den folgenden Abschnitten die verschiedenen Systemfaktoren aufgezeigt.

Festplatte

Für das Zwischenspeichern spielt Geschwindigkeit eine hohe Rolle. Man sollte sich also um diesen Faktor besonders kümmern. Bei Festplatten ist dieser Parameter als „zufällige Positionierzeit" in Millisekunden beschrieben. Als Faustregel gilt: Je niedriger dieser Wert, desto besser. Für eine hohe Geschwindigkeit empfiehlt es sich, schnelle Festplatten zu wählen.

Größe des Festplatten-Cache

In einem kleinen Cache ist die Wahrscheinlichkeit eines HIT (das gewünschte Objekt befindet sich bereits dort) sehr gering, da der Cache schnell gefüllt sein wird. In diesem Fall werden die selten gewünschten Objekte durch neue ersetzt. Steht jedoch `1 GB` für den Cache zur Verfügung und die Benutzer benötigen nur `10 MB` pro Tag zum Surfen, dann dauert es mehr als hundert Tage, bis der Cache voll ist.

Am leichtesten lässt sich die Größe des Cache durch die maximale Übertragungsrate der Verbindung bestimmen. Mit einer Verbindung von `1 MB/Sek` wird die maximale Übertragungsrate bei `125 KB/Sek` liegen. Landet der gesamte Datenverkehr im Cache, kommen innerhalb einer Stunde `450 MB` zusammen. Wenn man nun annimmt, dass der gesamte Datenverkehr lediglich während acht Arbeitsstunden erzeugt wird, erreicht man innerhalb eines Tages `3,6 GB`. Da die Verbindung nicht bis zur Kapazitätsgrenze ausgeschöpft wurde, konnten wir davon ausgehen, dass die gesamte Datenmenge, die durch den Cache geht, bei ungefähr `2 GB` liegt. In unserem Beispiel werden `2 GB` Speicher für Squid benötigt, um die Daten aller aufgerufenen Seiten *eines* Tages im Cache zu halten.

Zusammenfassend lässt sich sagen, dass Squid dazu tendiert, kleinere Datenblöcke von der Festplatte zu lesen oder darauf zu schreiben, so dass es wichtiger ist, wie schnell er diese Objekte auf der Festplatte findet, als eine Festplatte mit hohem Durchsatz zu haben.

RAM

Der von Squid benötigte Speicher ist abhängig von der Anzahl der im Cache zugewiesenen Objekte. Squid speichert Cache-Objektverweise und häufig angeforderte Objekte zusätzlich im Speicher, damit diese Daten schneller abgefragt werden können. Der Speicher ist eine Million mal schneller als eine Festplatte!

Squid hält auch andere Daten im Speicher, z. B. eine Tabelle mit allen vergebenen IP-Adressen, einen genau festgelegten Domainnamen-Cache, die am häufigsten gewünschten Objekte, Puffer, Zugriffskontrolllisten, etc.

Es ist sehr wichtig, dass ausreichend Speicher für den Squid-Prozess zur Verfügung steht. Sollte er auf Festplatte ausgelagert werden müssen, wird sich die Systemleistung nämlich drastisch reduzieren. Für die Cache-Speicherverwaltung wird das Tool cachemgr.cgi verwendet. Es wird im Abschnitt *cachemgr.cgi* auf Seite 362 erläutert.

CPU

Das Programm Squid benötigt nicht viel CPU. Nur beim Start und während der Überprüfung des Cache-Inhalts ist die Prozessorlast höher. Der Einsatz eines Multiprozessorrechners steigert nicht die Systemleistung. Zur Effektivitätssteigerung ist es besser, schnellere Festplatten zu verwenden oder mehr Speicher hinzuzufügen.

Einige Beispiele von konfigurierten Systemen, auf denen Squid läuft, finden sich unter `http://wwwcache.ja.net/servers/squids.html` .

Squid starten

Der Squid auf SuSE Linux ist bereits soweit vorkonfiguriert, dass man ihn problemlos sofort nach der Installation starten kann. Als Voraussetzung für einen reibungslosen Start sollte das Netzwerk soweit konfiguriert sein, dass mindestens ein Nameserver und sinnvollerweise auch das Internet erreichbar sind. Probleme kann es bereiten, wenn man eine Wählverbindung mit dynamischer DNS-Konfiguration verwendet. In so einem Fall sollte mindestens der Nameserver fest eingetragen sein, da Squid erst gar nicht startet, wenn er in der `/etc/resolv.conf` keinen DNS findet.

Um Squid zu starten, gibt man auf der Kommandozeile (als `root`)

```
rcsquid start
```

ein. Beim ersten Mal wird zunächst die Verzeichnisstruktur in `/var/squid/cache` angelegt. Dies wird vom Startskript `/etc/init.d/squid` automatisch durchgeführt und kann ein paar Sekunden bis Minuten dauern. Erscheint rechts in grün `done`, wurde Squid erfolgreich gestartet. Auf dem lokalen System kann man die Funktionsfähigkeit von Squid sofort testen, indem man im Browser als Proxy `localhost` und `Port 3128` einträgt. Um den Zugriff auf Squid und somit das Internet für alle zu ermöglichen, braucht man in der Konfigurationsdatei `/etc/squid.conf` lediglich den Eintrag `http_access deny all` auf `http_access allow all` zu ändern. Allerdings sollte man dabei bedenken, dass man den Squid damit komplett für jedermann öffnet. Von daher sollte man unbedingt ACLs definieren, die den Zugriff auf den Proxy regeln. Dazu mehr im Abschnitt *Optionen zur Zugriffskontrolle* auf Seite 356.

Hat man Änderungen an der Konfigurationsdatei `/etc/squid.conf` vorgenommen, muss man Squid dazu bringen, diese neu einzulesen. Das gelingt

mit:

```
rcsquid reload
```

Alternativ kann man Squid auch komplett neu starten:

```
rcsquid restart
```

Wichtig ist noch folgendes Kommando:

`rcsquid status` Damit kann man feststellen, ob der Proxy läuft und mit

```
rcsquid stop
```

wird Squid beendet. Letzteres kann eine Weile dauern, da Squid bis zu einer halben Minute (Option `shutdown_lifetime` in `/etc/squid.conf`) wartet, bevor die Verbindungen zu den Clients unterbrochen werden und er dann noch seine Daten auf Platte schreiben muss. Beendet man Squid mit einem `kill` oder `killall`, kann das einen zerstörten Cache zur Folge haben, den man dann löschen muss, um Squid wieder starten zu können.

Beendet sich Squid nach kurzer Zeit, obwohl er scheinbar erfolgreich gestartet wurde, kann das an einem fehlerhaften Nameserver-Eintrag oder einer fehlenden `/etc/resolv.conf` liegen. Den Grund für einen gescheiterten Start protokolliert Squid dabei in der Datei `/var/squid/logs/cache.log` . Soll Squid bereits beim Booten automatisch gestartet werden, muss im YaST2 Runlevel-Editor Squid für bestimmte Runlevel aktiviert werden.

Bei einer Deinstallation von Squid werden weder Cache noch Log-Dateien entfernt. Man muss das Verzeichnis `/var/cache/squid` manuell löschen.

Lokaler DNS-Server

Einen lokalen DNS-Server wie `BIND-8` oder `BIND-9` aufzusetzen, ist durchaus sinnvoll, auch wenn er keine eigene Domain verwaltet. Er fungiert dann lediglich als „Caching-only DNS“ und kann ohne spezielle Konfiguration DNS-Anfragen über die Root-Nameserver auflösen. Trägt man diesen in der `/etc/resolv.conf` mit der IP-Adresse `127.0.0.1` für `localhost` ein, findet Squid beim Starten immer einen gültigen Nameserver. Es reicht aus, das Paket zu installieren und BIND zu starten. Den Nameserver des Providers sollte man in der Konfigurationsdatei `/etc/named.conf` unter `forwarders` mit seiner IP-Adresse eintragen. Falls man eine Firewall laufen hat, und sei es nur die Personal-Firewall, muss man aber darauf achten, dass die DNS-Anfragen auch durchgelassen werden.

Die Konfigurationsdatei /etc/squid.conf

Alle Einstellungen zum Squid Proxyserver sind in der Datei `/etc/squid.conf` vorzunehmen. Um Squid erstmalig starten zu können, sind darin keine Änderungen erforderlich, der Zugriff von externen Clients ist jedoch erst einmal gesperrt. Für `localhost` ist der Proxy freigegeben und als Port wird standardmäßig `3128` verwendet. Die Optionen sind ausführlich und mit vielen Beispielen in der vorinstallierten `/etc/squid.conf` dokumentiert. Annähernd alle Einträge sind am Zeilenanfang durch ein #-Zeichen auskommentiert; am Zeilenende befinden sich die relevanten Spezifikationen. Die angegebenen Werte entsprechen fast immer den voreingestellten Werten, so dass das Entfernen des Kommentarzeichens, ohne den Parameter der Option zu ändern, bis auf wenige Ausnahmen keine Wirkung hat. Besser ist es, das Beispiel stehen zu lassen und die Option mit dem geänderten Parameter in der Zeile darunter neu einzufügen. So kann man die voreingestellten Werte und Änderungen problemlos nachvollziehen.

Hat man ein Update von einer älteren Squid-Version durchgeführt, ist es unbedingt zu empfehlen, die neue `/etc/squid.conf` zu verwenden und nur die Änderungen von der ursprünglichen Datei zu übernehmen. Versucht man die alte `squid.conf` weiter zu verwenden, läuft man Gefahr, dass die Konfiguration nicht mehr funktioniert, da Optionen immer wieder geändert werden und neue hinzukommen.

Allgemeine Konfigurations-Optionen

http_port 3128 Das ist der Port, auf dem Squid auf Anfragen der Clients lauscht. Voreingestellt ist `3128`, gebräuchlich ist auch `8080`. Es ist möglich, hier mehrere Portnummern, durch Leerzeichen getrennt, anzugeben.

cache_peer <hostname> <type> <proxy-port> <icp-port> Hier kann man einen übergeordneten Proxy als „Parent“ eintragen, z. B. wenn man den des Providers nutzen will oder muss. Als `<hostname>` trägt man den Namen bzw. die IP-Adresse des zu verwendenden Proxies und als `<type>` `parent` ein. Für `<proxy-port>` trägt man die Portnummer ein, die der Betreiber des Parent auch zur Verwendung im Browser angibt, meist `8080`. Den `<icp-port>` kann man auf `7` oder `0` setzen, wenn man den ICP-Port des Parent nicht kennt und die Benutzung dieses mit dem Provider nicht vereinbart wurde. Zusätzlich sollte man dann noch `default` und `no-query` nach den Portnummern angeben, um die Verwendung des ICP-Protokolls ganz zu unterbinden. Squid verhält sich dann gegenüber dem Proxy des Providers wie ein normaler Browser.

cache_mem 8 MB Dieser Eintrag gibt an, wie viel Arbeitsspeicher von Squid für das Cachen maximal verwendet wird. Voreingestellt sind `8 MB`.

cache_dir ufs /var/cache/squid 100 16 256 Der Eintrag `cache_dir` gibt das Verzeichnis an, in dem alle Objekte auf Platte abgelegt werden. Die Zahlen dahinter geben den maximal zu verwendenden Plattenplatz in `MB` und die Anzahl der Verzeichnisse in erster und zweiter Ebene an. Den Parameter `ufs` sollte man unverändert lassen. Voreingestellt sind `100 MB` Plattenplatz im Verzeichnis `/var/cache/squid` zu belegen und darin 16 Unterverzeichnisse anzulegen, die jeweils wiederum 256 Verzeichnisse enthalten. Bei Angabe des zu verwendenden Plattenplatzes sollte man genügend Reserven lassen, sinnvoll sind Werte zwischen 50 und maximal 80 Prozent des verfügbaren Platzes. Die beiden letzten Zahlen für die Anzahl der Verzeichnisse sollte man nur mit Vorsicht vergrößern, da zu viele Verzeichnisse auch wieder auf Kosten der Performance gehen können. Hat man mehrere Platten, auf die der Cache verteilt werden soll, kann man entsprechend viele `cache_dir`-Zeilen eintragen.

cache_access_log /var/squid/logs/access.log Pfadangabe für Log-Dateien.

cache_log /var/squid/logs/cache.log Pfadangabe für Log-Dateien.

cache_store_log /var/squid/logs/store.log Pfadangabe für Log-Dateien. Diese drei Einträge geben den Pfad zur Protokolldatei von Squid an. Normalerweise wird man daran nichts ändern. Wird der Squid stark beansprucht, kann es sinnvoll sein, den Cache und die Log-Dateien auf verschiedene Platten zu legen.

emulate_httpd_log off Ändert man diesen Eintrag auf `on`, erhält man lesbare Log-Dateien. Allerdings kommen manche Auswerteprogramme damit nicht zurecht.

client_netmask 255.255.255.255 Mit diesem Eintrag kann man die protokollierten IP-Adressen in den Log-Dateien maskieren, um die Identität der Clients zu verbergen. Trägt man hier `255.255.255.0` ein, wird die letzte Stelle der IP-Adresse auf Null gesetzt.

ftp_user Squid@do.main Hiermit kann man das Passwort setzen, welches Squid für den anonymen FTP-Login verwenden soll. Es kann aber sinnvoll sein, hier eine gültige E-Mail-Adresse in der eigenen Domain anzugeben, da einige FTP-Server diese auf Gültigkeit überprüfen.

cache_mgr webmaster Eine E-Mail-Adresse, an die Squid eine Nachricht schickt, wenn er unerwartet abstürzt. Voreingestellt ist `webmaster`.

logfile_rotate 0 Squid ist in der Lage, die gesicherten Log-Dateien zu rotieren, wenn man `squid -k rotate` aufruft. Die Dateien werden dabei, entsprechend der angegebenen Anzahl, durchnummeriert, und nach Erreichen des angegebenen Wertes wird die jeweils älteste Datei wieder überschrieben. Dieser Wert steht standardmäßig auf `0`, weil das Archivieren und Löschen der Log-Dateien bei SuSE Linux von einem eigenen Cronjob durchgeführt wird, dessen Konfiguration man in der Datei `/etc/logrotate/syslog` findet. Der Zeitraum, nach dem die Dateien gelöscht werden, wird in der Datei `/etc/sysconfig/aaa_base` mit dem Eintrag `MAX_DAYS_FOR_LOG_FILES` festgelegt.

append_domain <domain> Mit `append_domain` kann man angeben, welche Domain automatisch angehängt wird, wenn keine angegeben wurde. Meist wird man hier die eigene Domain eintragen, dann genügt es, im Browser `www` einzugeben, um auf den eigenen Webserver zu gelangen.

forwarded_for on Setzt man diesen Eintrag auf `off`, entfernt Squid die IP-Adresse bzw. den Systemnamen des Clients aus den HTTP-Anfragen.

negative_ttl 5 minutes; negative_dns_ttl 5 minutes Normalerweise braucht man diese Werte nicht zu verändern. Hat man aber eine Wählleitung, kann es vorkommen, dass das Internet zeitweilig nicht erreichbar ist. Squid merkt sich dann die erfolglosen Anfragen und weigert sich, diese neu anzufragen, obwohl die Verbindung in das Internet wieder steht. Für diesen Fall sollte man die `minutes` in `seconds` ändern, dann führt auch ein `Reload` im Browser, wenige Sekunden nach der Einwahl, wieder zum Erfolg.

never_direct allow <acl_name> Will man verhindern, dass Squid Anfragen direkt aus dem Internet fordert, kann man hiermit die Verwendung eines anderen Proxies erzwingen. Diesen muss man zuvor unter `cache_peer` eingetragen haben. Gibt man als `<acl_name> all` an, erzwingt man, dass sämtliche Anfragen direkt an den `parent` weitergegeben werden. Das kann zum Beispiel nötig sein, wenn man einen Provider verwendet, der die Verwendung seines Proxies zwingend vorschreibt oder die Firewall keinen direkten Zugriff auf das Internet durchlässt.

Optionen zur Zugriffskontrolle

Squid bietet ein ausgeklügeltes System, um den Zugriff auf den Proxy zu steuern. Durch die Verwendung von ACLs ist es einfach und vielseitig konfigurierbar. Dabei handelt es sich um Listen mit Regeln, die der Reihe nach

abgearbeitet werden. ACLs müssen zuerst definiert werden, bevor sie verwendet werden können. Einige Standard-ACLs wie `all` und `localhost` sind bereits vorhanden. Das Festlegen einer ACL an sich bewirkt aber noch gar nichts. Erst wenn sie tatsächlich eingesetzt wird, z. B. in Verbindung mit `http_access`, werden die definierten Regeln abgearbeitet.

acl <acl_name> <type> <data> Eine ACL benötigt zur Definition mindestens drei Angaben. Der Name `<acl_name>` kann frei gewählt werden. Für `<type>` kann man aus einer Vielzahl unterschiedlicher Möglichkeiten auswählen, die man im Abschnitt `ACCESS CONTROLS` in der `/etc/squid.conf` nachlesen kann. Was für `<data>` anzugeben ist, hängt vom jeweiligen Typ der ACL ab und kann auch aus einer Datei, z. B. mit Rechnernamen, IP-Adressen oder URLs eingelesen werden. Im folgenden einige einfache Beispiele:

```
acl meinesurfer srcdomain .meine-domain.com
acl lehrer src 192.168.1.0/255.255.255.0
acl studenten src 192.168.7.0-192.168.9.0/255.255.255.0
acl mittags time MTWHF 12:00-15:00
```

http_access allow <acl_name> Mit `http_access` wird festgelegt, wer den Proxy verwenden darf und auf was er im Internet zugreifen darf. Dabei sind ACLs anzugeben, `localhost` und `all` sind weiter oben bereits definiert, die mit `deny` oder `allow` den Zugriff sperren oder freigeben. Man kann hier eine Liste mit vielen `http_access`-Einträgen erstellen, die von oben nach unten abgearbeitet werden; je nachdem, was zuerst zutrifft, wird der Zugriff auf die angeforderte URL freigegeben oder gesperrt. Als letzter Eintrag sollte immer `http_access deny all` stehen. Im folgenden Beispiel hat `localhost`, also der lokale Rechner, freien Zugriff auf alles, während er für alle anderen komplett gesperrt ist:

```
http_access allow localhost
http_access deny all
```

Noch ein Beispiel, in dem die zuvor definierten ACLs verwendet werden: Die Gruppe `lehrer` hat jederzeit Zugriff auf das Internet, während die Gruppe `studenten` nur Montags bis Freitags, und da nur mittags, surfen darf:

```
http_access deny localhost
```

```
http_access allow lehrer
http_access allow studenten mittags
http_access deny all
```

Die Liste mit den eigenen `http_access`-Einträgen sollte man der Übersichtlichkeit halber nur an der dafür vorgesehenen Stelle in der `/etc/squid.conf` eintragen. Das bedeutet zwischen dem Text

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

und dem abschließenden

```
http_access deny all
```

redirect_program /usr/bin/squidGuard Mit dieser Option kann man einen „Redirector", wie z. B. SquidGuard angeben, der in der Lage ist, unerwünschte URLs zu sperren. In Verbindung mit Proxy-Authentifizierung und den passenden ACLs kann man so den Zugriff auf das Internet für verschiedene Benutzergruppen sehr differenziert steuern. SquidGuard ist ein eigenes Paket, das separat zu installieren und konfigurieren ist.

authenticate_program /usr/sbin/pam_auth Sollen sich die Benutzer am Proxy authentifizieren müssen, kann man hier ein entsprechendes Programm wie z. B. pam_auth angeben. Bei der Verwendung von pam_auth öffnet sich für den Anwender beim ersten Zugriff ein Loginfenster, in dem er Benutzername und Passwort eingeben muss. Zusätzlich ist noch eine ACL erforderlich, damit nur Clients mit gültigem Login surfen können:

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

Das `REQUIRED` nach `proxy_auth` kann man auch durch eine Liste von erlaubten Benutzernamen oder einen Pfad zu solch einer Liste ersetzen.

ident_lookup_access allow <acl_name> Hiermit erreicht man, dass auf alle durch die ACL definierten Clients eine Ident-Anfrage ausgeführt wird, um die Identität des jeweiligen Benutzers zu ermitteln. Setzt man für `<acl_name>` `all` ein, erfolgt dies generell für alle Clients. Auf den Clients muss dazu ein Ident-Daemon laufen, bei Linux kann man dafür

das Paket pidentd installieren, für Windows gibt es freie Software, die man sich aus dem Internet besorgen kann. Damit nur Clients mit erfolgreichem Ident-Lookup zugelassen werden, ist auch hier wieder eine entsprechende ACL zu definieren:

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

Auch hier kann man das REQUIRED wieder durch eine Liste erlaubter Benutzernamen ersetzen. Die Verwendung von Ident kann den Zugriff merklich verlangsamen, da die Ident-Lookups durchaus für jede Anfrage wiederholt werden.

Transparente Proxy-Konfiguration

Normalerweise schickt der Web-Browser an einen bestimmten Port des Proxy-Servers Anfragen und der Proxy stellt die angeforderten Objekte zur Verfügung, ob sie nun im Cache sind oder nicht. Innerhalb eines echten Netzwerks können verschiedene Situationen auftreten:

- Aus Sicherheitsgründen ist es besser, wenn alle Clients zum Surfen im Internet einen Proxy verwenden.
- Es ist notwendig, dass alle Clients einen Proxy verwenden, egal ob sie sich dessen bewusst sind oder nicht.
- In großen Netzwerken, die bereits einen Proxy verwenden, ist es möglich, veränderte Konfigurationen der einzelnen Rechner zu speichern, falls sich Änderungen am System ergeben.

In jedem dieser Fälle kann ein transparenter Proxy eingesetzt werden.
Das Prinzip ist denkbar einfach: Der Proxy nimmt die Anfragen des Web-Browsers entgegen und bearbeitet sie, sodass der Web-Browser die angeforderten Seiten erhält ohne zu wissen, woher sie kommen. Der gesamte Prozess wird transparent ausgeführt, daher der Name für den Vorgang.

Kernel-Konfiguration

Zuerst sollte sicherstellt sein, dass der Kernel des Proxy-Servers einen transparenten Proxy unterstützt. Andernfalls muss man dem Kernel diese Optionen hinzufügen und ihn neu kompilieren. Genauere Informationen dazu entnehmen Sie bitte dem Kapitel *Der Linux Kernel* auf Seite 185.

Kernel Module verändern sich von Version zu Version. Prüfen Sie den aktuellen Stand unter `/usr/share/doc/howto/en/html/mini/TransparentProxy-3.html` bzw. im Internet: `http://www.tldp.org/HOWTO/mini/TransparentProxy-3.html`.

Nun müssen Sie nur noch die neue Konfiguration speichern, den neuen Kernel kompilieren und installieren; ggf. muss auch LILO neu konfiguriert werden. Anschließend muss das System neu gestartet werden.

Konfigurationsoptionen in /etc/squid.conf

Folgende Optionen in der Datei `/etc/squid.conf` müssen aktiviert werden, um einen transparenten Proxy aufzusetzen:

- `httpd_accel_host` virtual
- `httpd_accel_port` 80 # Port, auf dem sich der tatsächliche HTTP-Server befindet.
- `httpd_accel_with_proxy` on
- `httpd_accel_uses_host_header` on

Firewall-Konfiguration mit SuSEfirewall2

Alle durch die Firewall eingehenden Anfragen müssen mithilfe einer Port-Weiterleitungsregel an den Squid-Port weitergeleitet werden.

Dafür eignet sich das SuSE-eigenes Tool SuSEfirewall2. Dessen Konfigurationsdatei findet man in der Datei `/etc/sysconfig/scripts/SuSEfirewall2-custom`. Die Konfigurationsdatei wiederum setzt sich aus gut dokumentierten Einträgen zusammen. Auch wenn wir nur einen transparenten Proxy einrichten wollen, müssen wir einige Firewall-Optionen konfigurieren. Beispielsweise:

- Gerät zeigt auf Internet: `FW_DEV_WORLD`="eth1"
- Gerät zeigt auf Netzwerk: `FW_DEV_INT`="eth0"

Auf Ports und Dienste (siehe `/etc/exports`) in der Firewall wird von nicht vertrauenswürdigen Netzwerken also dem Internet zugegriffen. In diesem Beispiel bieten wir lediglich Web-Dienste nach außen hin an:

`FW_SERVICES_EXTERNAL_TCP`="www"

Auf Ports/Dienste (siehe `/etc/exports`) in der Firewall wird vom sicheren Netzwerk, sowohl TCP und UDP, zugegriffen.

`FW_SERVICES_INTERNAL_TCP`="domain www 3128"

`FW_SERVICES_INTERNAL_UDP`="domain"

Wir greifen auf Web-Dienste und Squid (dessen Standardport ist 3128) zu. Der oben beschriebene Dienst „Domain“ steht für DNS oder Domain Name Server. Es ist üblich, diesen Dienst zu nutzen. Andernfalls entfernen wir ihn einfach aus obigem Eintrag und setzen folgende Option auf `no`:

`FW_SERVICE_DNS`="yes"

Die wichtigste Option ist die Ziffer 15:

```
#
# 15.)
# Welcher Zugriff auf die einzelnen Dienste soll an einen lokalen
# Port auf dem Firewall-Rechner umgeleitet werden?
#
# Damit können alle internen Benutzer gezwungen werden, über den
# Squid-Proxy zu surfen oder es kann eingehender Webverkehr
# transparent an einen sicheren Web-Server umgeleitet werden.
#
# Wahl: keinen Eintrag vornehmen oder folgend erklärte Syntax von
# Umleitungsregeln, getrennt durch Leerzeichen, verwenden.
# Eine Umleitungsregel besteht aus 1) Quelle IP/Netz, 2) Ziel
# IP/Netz, 3) ursprünglicher Zielport und 4) lokaler Port, an den
# der Verkehr umgeleitet werden soll, getrennt durch Kommata, z.~B.:
# "10.0.0.0/8,0/0,80,3128 0/0,172.20.1.1,80,8080"
#
```

Datei 36: *Option 15 der Firewallkonfiguration*

Im obigen Kommentar wird die einzuhaltende Syntax gezeigt. Zuerst greifen die IP-Adresse und die Netzwerkmaske der „internen Netzwerke“ auf die Proxy-Firewall zu. Dann die IP-Adresse und die Netzwerkmaske, an die Anfragen von den Clients „gesendet“ werden. Im Fall von Web-Browsern wählt man die Netzwerke `0/0`. Dies ist eine Wildcard und bedeutet „überallhin“.

Danach kommt der „ursprüngliche“ Port, an den diese Anfragen geschickt wurden und schließlich folgt der Port, an den die Anfragen „umgeleitet“ wurden.

Da Squid mehr Protokolle unterstützt als nur HTTP, können auch Anfragen von anderen Ports an den Proxy umgeleitet werden, so zum Beispiel FTP (Port 21), HTTPS oder SSL (Port 443).

Im konkreten Fall werden Web-Dienste (Port `80`) auf den Proxy-Port (hier `3128` umgeleitet. Falls mehrere Netzwerke oder Dienste hinzugefügt werden sollen, müssen diese durch ein Leerzeichen im entsprechenden Eintrag getrennt werden.

`FW_REDIRECT_TCP`="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"

`FW_REDIRECT_UDP`="192.168.0.0/16,0/0,80,3128 192.168.0.0/16,0/0,21,3128"

Zum Starten der Firewall und der neuen Konfiguration muss man einen Eintrag in der Datei `/etc/sysconfig/SuSEfirewall2` editieren. Der Eintrag `START_FW` muss auf "yes"gesetzt werden:

Starten Sie Squid wie in Abschnitt *Squid starten* auf Seite 352 beschrieben. Anhand der Protokolldateien in `/var/log/squid/access.log` kann überprüft werden, ob alles richtig funktioniert. Um zu überprüfen, ob alle Ports korrekt konfiguriert wurden, kann von jedem beliebigen Rechner außerhalb unserer Netzwerke auf dem Rechner ein Portscan ausgeführt werden. Nur der Web-Dienst-Port (80) solte offen sein. Der Portscan führt über `nmap`:

```
nmap -O IP_address
```

Squid und andere Programme

In diesem Abschnitt wird gezeigt, wie andere Applikationen mit Squid interagieren.

cachemgr.cgi ermöglicht dem Systemadministrator, den benötigten Speicher für das Zwischenspeichern von Objekten zu überprüfen. Squidgrd filtert Webseiten, und calamaris ist ein Berichtsgenerator für Squid.

cachemgr.cgi

Der Cache-Manager (cachemgr.cgi) ist ein CGI-Hilfsprogramm zur Ausgabe von Statistiken über den benötigten Speicher des laufenden Squid-Prozesses. Im Gegensatz zum Protokollieren erleichtert dies die Cache-Verwaltung und die Anzeige von Statistiken.

Einrichten

Zuerst wird ein lauffähiger Web-Server auf dem System benötigt. Als Benutzer `root` gibt man Folgendes ein, um herauszufinden, ob Apache bereits läuft: `rcapache status`.

Erscheint eine Nachricht wie diese:

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

dann läuft Apache auf unserem Rechner. Andernfalls müssen Sie Folgendes eingeben: `rcapache start`

So wird Apache mit den SuSE Linux-Standardeinstellungen gestartet. Weitere Details zu Apache finden sich in diesem Handbuch.

Als letzten Schritt muss man die Datei `cachemgr.cgi` in das Verzeichnis `cgi-bin` von Apache kopieren:

```
cp /usr/share/doc/packages/squid/scripts/cachemgr.cgi
/usr/local/httpd/cgi-bin
```

Cache-Manager ACLs in /etc/squid.conf

Folgende Standardeinstellungen sind für den Cache-Manager erforderlich:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

Folgende Regeln sollten enthalten sein:

```
http_access allow manager localhost
http_access deny manager
```

Die erste ACL ist am wichtigsten, da der Cache-Manager versucht, mit dem Squid über das cach_object-Protokoll zu kommunizieren. Die folgenden Regeln setzen voraus, dass der Web-Server und Squid auf demselben Rechner laufen. Die Kommunikation zwischen dem Cache-Manager und Squid entsteht beim Web-Server, nicht beim Browser. Befindet sich der Web-Server also auf einem anderen Rechner, müssen Sie extra eine ACL wie in der Beispieldatei 37 auf der nächsten Seite hinzufügen.

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # IP Webserver
```

Datei 37: *Zugriffsregeln*

Dann werden noch folgende Regeln aus Datei 38 benötigt.

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

Datei 38: *Zugriffsregeln*

Es ist auch möglich, ein Passwort für den Manager zu konfigurieren, wenn auf mehrere Optionen zugegriffen werden soll, wie z. B. Schließen des Cache von Remote oder Anzeigen weiterer Informationen über den Cache. Dann müssen Sie den Eintrag `cachemgr_passwd` und die Optionenliste, die angezeigt werden soll, mit einem Passwort für den Manager konfigurieren. Diese Liste erscheint als Teil der Eintragkommentare in `/etc/squid.conf`.

Immer wenn sich die Konfigurationsdatei geändert hat, muss Squid mit der Option `-k reconfigure` neu gestartet werden.

Statistiken anzeigen

Gehen Sie zur entsprechenden Web-Seite, z. B.:
`http://webserver.example.org/cgi-bin/cachemgr.cgi`

Drücken Sie auf 'continue' und lassen Sie sich die verschiedenen Statistiken anzeigen. Weitere Informationen über die einzelnen Einträge, die vom Cache-Manager ausgegeben werden, finden sich in den FAQs zu Squid: `http://www.squid-cache.org/Doc/FAQ/FAQ-9.html`

SquidGuard

Dieses Kapitel soll lediglich eine Einführung zur Konfiguration von SquidGuard sowie ein paar Ratschläge zu dessen Einsatz geben. Auf eine umfangreiche Erklärung wird an dieser Stelle verzichtet. Tiefer gehende Informationen finden sich auf den Webseiten zu SquidGuard: `http://www.squidguard.org`

SquidGuard ist ein freier (GPL), flexibler und ultraschneller Filter, ein Umleiter und „Zugriffs-Controller-PlugIn" für Squid. Er ermöglicht das Festlegen

einer Vielzahl von Zugriffsregeln mit unterschiedlichen Beschränkungen für verschiedene Benutzergruppen für einen Squid-Cache. SquidGuard verwendet die Standardschnittstelle von Squid zum Umleiten.

squidGuard kann u. a. für Folgendes verwendet werden:

- Beschränkung des Internetzugriffs für einige Benutzer auf bestimmte akzeptierte/bekannte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf bestimmte Web-Server und/oder URLs.
- Zugriffsverweigerung für einige Benutzer auf URLs, die bestimmte reguläre Ausdrücke oder Wörter enthalten.
- Umleiten gesperrter URLs an eine „intelligente" CGI-basierte Infoseite.
- Umleiten nicht registrierter Benutzer an ein Registrationsformular.
- Umleiten von Bannern an ein leeres GIF.
- Unterschiedliche Zugriffsregeln abhängig von der Uhrzeit, dem Wochentag, dem Datum etc.
- Unterschiedliche Regeln für die einzelnen Benutzergruppen.

Weder mit squidGuard noch mit Squid ist Folgendes möglich:

- Text innerhalb von Dokumenten filtern, zensieren oder editieren.
- In HTML eingebettete Skriptsprachen wie JavaScript oder VBscript filtern, zensieren oder editieren.

Verwendung von SquidGuard

Installieren Sie das Paket `squidgrd`. Editieren Sie die Konfigurationsdatei `/etc/squidguard.conf`. Es gibt zahlreiche andere Konfigurationsbeispiele unter `http://www.squidguard.org/config/`. Sie können später mit komplizierteren Konfigurationsenstellungen experimentieren.

Der nächste Schritt besteht darin, eine Dummy-Seite „Zugriff verweigert" oder eine mehr oder weniger intelligente CGI-Seite zu erzeugen, um Squid umzuleiten, falls der Client eine verbotene Webseite anfordert. Der Einsatz von Apache wird auch hier wieder empfohlen.

Nun müssen wir Squid sagen, dass er SquidGuard benutzen soll. Dafür verwenden wir folgende Einträge in der Datei `/etc/squid.conf`:

```
redirect_program /usr/bin/squidGuard
```

Eine andere Option namens `redirect_children` konfiguriert die Anzahl der verschiedenen auf dem Rechner laufenden „redirect“, also Umleitungsprozesse (in diesem Fall SquidGuard). SquidGuard ist schnell genug, um eine Vielzahl von Anfragen (SquidGuard ist wirklich schnell: 100.000 Anfragen innerhalb von 10 Sekunden auf einem 500MHz Pentium mit 5900 Domains, 7880 URLs,gesamt 13780) zu bearbeiten. Es wird daher nicht empfohlen, mehr als 4 Prozesse festzusetzen, da die Zuweisung dieser Prozesse unnötig viel Speicher braucht.

```
redirect_children 4
```

Als Letztes senden Sie ein HUP-Signal zum Squid, damit die neue Konfiguration eingelesen wird:

```
squid -k reconfigure
```

Nun können Sie Ihre Einstellungen in einem Browser testen.

Erzeugen von Cache-Berichten mit Calamaris

Calamaris ist ein Perl-Skript, das zur Erzeugung von Aktivitätsberichten des Cache im ASCII- oder HTML-Format verwendet wird. Es arbeitet mit Squid-eigenen Zugriffsprotokolldateien. Die Homepage zu Calamaris befindet sich unter: `http://Calamaris.Cord.de/`

Das Programm ist einfach zu verwenden. Melden Sie sich als `root` an und geben Sie Folgendes ein:

```
cat access.log.files | calamaris [options] > reportfile
```

Beim Verketten mehrerer Protokolldateien ist die Beachtung der chronologischen Reihenfolge wichtig, d. h. ältere Dateien kommen zuerst.

Die verschiedenen Optionen:

-a wird normalerweise zur Ausgabe aller verfügbaren Berichte verwendet, mit

-w erhält man einen HTML-Bericht und mit

-l eine Nachricht oder ein Logo im Header des Berichts.

Weitere Informationen über die verschiedenen Optionen finden Sie in der Manual Page zu calamaris: `man calamaris`

Ein übliches Beispiel:

```
cat access.log.2 access.log.1 access.log | calamaris -a -w \
```

```
>/usr/local/httpd/htdocs/Squid/squidreport.html
```

Der Bericht wird im Verzeichnis des Web-Servers abgelegt. Wieder wird Apache benötigt, um die Berichte anzeigen zu können.

Ein weiteres, leistungsstarkes Tool zum Erzeugen von Cache-Berichten ist SARG (Squid Analysis Report Generator). Weitere Informationen dazu gibt es auf der entsprechenden Internetseite unter: `http://web.onda.com.br/orso/`

Weitere Informationen zu Squid

Besuchen Sie die Homepage von Squid: `http://www.squid-cache.org/`. Hier finden Sie den Squid User Guide und eine sehr umfangreiche Sammlung von FAQs zu Squid.

Das Mini-Howto zu einem transparenten Proxy im Paket `howtoen`, unter: `/usr/share/doc/howto/en/mini/TransparentProxy.gz`

Des Weiteren gibt es Mailinglisten für Squid unter: `squid-users@squid-cache.org`.

Das Archiv dazu befindet sich unter: `http://www.squid-cache.org/mail-archive/squid-users/`

Teil V

Anhänge

Dateisysteme unter Linux

Linux unterstützt eine ganze Reihe von Dateisystemen. Dieses Kapitel gibt einen kurzen Überblick über die bekanntesten Dateisysteme unter Linux, wobei wir insbesondere auf deren Designkonzept und Vorzüge sowie auf die Bandbreite der Programme eingehen werden. Weiterhin werden einige Informationen zum „Large File Support“ unter Linux bereitgestellt.

Glossar

Metadaten Die interne Datenstruktur eines Dateisystems, die eine geordnete Struktur und die Verfügbarkeit der Festplattendaten gewährleistet. Im Grunde genommen sind es die „Daten über die Daten“. Nahezu jedes Dateisystem besitzt seine eigene Metadatenstruktur. Hierin liegt zum Teil auch der Grund für die unterschiedlichen Leistungsmerkmale der verschiedenen Dateisysteme. Es ist von äußerster Wichtigkeit, die Metadaten intakt zu halten, da andernfalls das gesamte Dateisystem zerstört werden könnte.

Inode Inodes enthalten alle möglichen Informationen über eine Datei, wie den Namen, die Größe, die Anzahl der Links, Datum, Erstellungszeit, Änderungen, Zugriff sowie Zeiger (engl. *pointer*) auf die Festplattenblöcke, wo die Datei gespeichert ist.

Journal Im Zusammenhang mit einem Dateisystem ist ein Journal eine platteninterne Struktur mit einer Art Protokoll, in das der Dateisystemtreiber die zu ändernden (Meta-)daten des Dateisystems einträgt. „Journaling“ verringert die Wiederherstellungszeit eines Linux-Systems enorm, da der Dateisystemtreiber keine umfassende Suche nach zerstörten Metadaten auf der gesamten Platte starten muss. Stattdessen werden die Journal-Einträge wieder eingespielt.

Die wichtigsten Dateisysteme unter Linux

Anders als noch vor zwei oder drei Jahren ist die Auswahl eines Dateisystems für Linux nicht mehr eine Angelegenheit von Sekunden („Ext2 oder ReiserFS?“). Kernel ab der Version 2.4 bieten eine große Auswahl an Dateisystemen. Im Folgenden erhalten Sie einen groben Überblick über die grundlegende Funktionsweise dieser Dateisysteme und deren Vorteile.

Seien Sie sich immer bewusst, dass kein Dateisystem allen Applikationen gleichermaßen gerecht werden kann. Jedes Dateisystem hat seine ihm eigenen Stärken und Schwächen, die berücksichtigt werden müssen. Sogar das hochentwickeltste Dateisystem der Welt wird niemals ein vernünftiges Backupkonzept ersetzen.

Die Fachbegriffe „Datenintegrität“ oder „Datenkonsistenz“ beziehen sich in diesem Kapitel nicht auf die Konsistenz der Speicherdaten eines Benutzers (diejenigen Daten, die Ihre Applikation in ihre Dateien schreibt). Die Konsistenz dieser Daten muss von der Applikation selbst gewährleistet werden.

Ext2

Die Ursprünge von Ext2 finden sich in der frühen Geschichte von Linux. Sein Vorgänger, das Extended File System, wurde im April 1992 implementiert und in Linux 0.96c integriert. Das Extended File System erfuhr eine Reihe von Änderungen und wurde für Jahre als Ext2 das bekannteste Dateisystem unter Linux. Mit dem Einzug der Journaling File Systeme und deren erstaunlich kurzen Wiederherstellungszeiten verlor Ext2 an Wichtigkeit.

Möglicherweise hilft Ihnen eine kurze Zusammenfassung der Stärken von Ext2 beim Verständnis für dessen Beliebtheit unter den Linux-Benutzern, die es teilweise noch heute als Dateisystem bevorzugen.

Stabilität Als wahrer „old-timer“, erfuhr Ext2 viele Verbesserungen und wurde ausführlich getestet. Daher wohl auch sein Ruf als „rock–solid“. Im Falle eines Systemausfalls, bei dem das Dateisystem nicht sauber ungemountet werden konnte, startet e2fsck eine Analyse der Dateisystemdaten. Metadaten werden in einen konsistenten Zustand gebracht und schwebende Dateien oder Datenblöcke werden in ein ausgewiesenes Verzeichnis geschrieben (genannt `lost+found`). Im Gegensatz zu (den meisten) Journaling File Systemen analysiert e2fsck das gesamte Dateisystem und nicht nur die kürzlich veränderten Metadatenbits. Dies dauert bedeutend länger als die Überprüfung der Protokolldaten eines Journaling File Systems. Je nach Größe des Dateisystems kann dies eine

halbe Stunde und mehr in Anspruch nehmen. Deshalb werden Sie Ext2 für keinen Server wählen, der hochverfügbar sein muss. Da Ext2 jedoch kein Journal pflegen muss und bedeutend weniger Speicher verbraucht, ist es manchmal schneller als andere Dateisysteme.

Leichtes Upgrade Basierend auf dem starken Fundament Ext2 konnte sich Ext3 zu einem gefeierten Dateisystem der nächsten Generation entwickeln. Seine Zuverlässigkeit und Stabilität wurden geschickt mit den Vorzügen eines Journaling File Systems verbunden.

Ext3

Ext3 wurde von Stephen Tweedie entworfen. Anders als alle anderen „next-generation" Dateisysteme, folgt Ext3 keinem komplett neuen Designprinzip. Es basiert auf Ext2. Diese beiden Dateisysteme sind sehr eng miteinander verwandt. Ein Ext3-Dateisystem kann leicht auf einem Ext2-Dateisystem aufgebaut werden. Der grundlegendste Unterschied zwischen Ext2 und Ext3 liegt darin, dass Ext3 Journaling unterstützt.

Zusammenfassend lassen sich für Ext3 drei Vorteile herausstellen:

Leichte und höchst zuverlässige Dateisystem-Upgrades von Ext2 Da Ext3 auf dem Ext2-Code basiert und sowohl sein platteneigenes Format als auch sein Metadatenformat teilt, sind Upgrades von Ext2 auf Ext3 sehr unkompliziert. Sie können sogar dann durchgeführt werden, wenn Ihre Ext2-Dateisysteme gemountet sind. Anders als beim Umstieg auf andere Journaling File Systeme, wie z.B. ReiserFS, JFS, oder XFS, der sehr mühsam sein kann, (sie müssen Sicherungskopien des gesamten Dateisystems erstellen und dieses anschließend von Grund auf neu erstellen), ist ein Umstieg auf Ext3 eine Angelegenheit von Minuten. Zugleich ist er sehr sicher, da die Wiederherstellung eines gesamten Dateisystems von Grund auf nicht immer fehlerlos vonstatten geht. Betrachtet man die Anzahl der vorhandenen Ext2-Systeme, die auf ein Upgrade auf ein Journaling File System warten, kann man sich leicht die Bedeutung von Ext3 für viele Systemadministratoren ausmalen. Ein Downgrade von Ext3 auf Ext2 ist genauso leicht wie das Upgrade. Führen Sie einfach einen sauberen Unmount des Ext3-Dateisystems durch und mounten Sie es als ein Ext2-Dateisystem.

Zuverlässigkeit und Performance Andere Journaling File Systeme folgen dem „metadata-only"-Journaling-Ansatz. Das heißt, Ihre Metadaten bleiben in einem konsistenten Zustand; dies kann jedoch nicht automatisch

für die Dateisystemdaten selbst garantiert werden. Ext3 ist in der Lage, sich sowohl um die Metadaten als auch die Daten selbst zu kümmern. Wie eingehend sich Ext3 um Daten und Metadaten kümmert, ist individuell einstellbar. Den höchsten Grad an Sicherheit (d.h. Datenintegrität) erreicht man durch den Start von Ext3 im `data=journal`-Modus; dies jedoch kann das System verlangsamen, da sowohl Metadaten als auch Daten selbst im Journal erfasst werden. Ein relativ neuer Ansatz besteht in der Verwendung des `data=ordered`-Modus, der sowohl die Daten- als auch die Metadatenintegrität gewährleistet, jedoch das Journaling nur für Metadaten verwendet. Der Dateisystemtreiber sammelt alle Datenblöcke, die zu einem Metadaten-Update gehören. Diese Blöcke werden als „transaction" gruppiert und werden auf die Platte geschrieben, bevor die Metadaten aktualisiert sind. Somit erreicht man Metadaten- und Datenkonsistenz ohne Leistungsverlust. Eine dritte Verwendungsart ist `data=writeback`. Hierbei können Daten in das Hauptdateisystem geschrieben werden, nachdem ihre Metadaten an das Journal übergeben wurden. Diese Option ist nach Meinung vieler aus Performancegründen die beste Einstellung. Jedoch kann es bei dieser Option passieren, dass alte Daten nach einem Absturz und einer Wiederherstellung in Dateien auftauchen, während die interne Dateisystemintegrität gewahrt wird. Sofern nicht anders angegeben, wird Ext3 mit der Standardeinstellung `data=ordered` gestartet.

ReiserFS

Offiziell stand eine der Hauptfunktionen der Kernel-Version 2.4, ReiserFS seit der SuSE Linux-Version 6.4 als Kernel-Patch für 2.2.x SuSE-Kernel zur Verfügung. ReiserFS stammt von Hans Reiser und dem Namesys-Entwicklungsteam. ReiserFS hat sich als mächtige Alternative zu Ext2 profiliert. Seine größten Vorteile sind bessere Festplattenspeicherverwaltung, bessere Plattenzugriffsleistung und schnellere Wiederherstellung nach Abstürzen. Einen kleinen Wermutstropfen gibt es dennoch: ReiserFS legt großen Wert auf die Metadaten, jedoch nicht auf die Daten selbst. Die nächsten Generationen von ReiserFS werden Data-Journaling beinhalten (sowohl Metadaten als auch tatsächliche Daten werden in das Journal geschrieben) sowie geordnete Schreibzugriffe (siehe `data=ordered` unter Ext3).

Die Stärken von ReiserFS im Detail:

Bessere Festplattenspeicherverwaltung In ReiserFS werden alle Daten in einer Struktur namens B*-balanced tree organisiert. Die Baumstruktur

trägt zur besseren Festplattenspeicherverwaltung bei, da kleine Dateien direkt in den Blättern des B*trees gespeichert werden können, statt sie an anderer Stelle zu speichern und einfach den Zeiger auf den tatsächlichen Ort zu verwalten. Zusätzlich dazu wird der Speicher nicht in Einheiten von 1 oder 4 kB zugewiesen, sondern in exakt der benötigten Einheit. Ein weiterer Vorteil liegt in der dynamischen Vergabe von Inodes. Dies verschafft dem Dateisystem eine größere Flexibilität gegenüber herkömmlichen Dateisystemen, wie z.B. Ext2, wo die Inode-Dichte zum Zeitpunkt der Erstellung des Dateisystems angegeben werden muss.

Bessere Festplattenzugriffsleistung Bei kleinen Dateien werden Sie häufig bemerken können, dass sowohl die Dateidaten als auch die „stat_data" (Inode)-Informationen nebeneinander gespeichert wurden. Ein einziger Festplattenzugriff reicht somit, um Sie mit allen benötigten Informationen zu versorgen.

Schnelle Wiederherstellung nach Abstürzen Durch den Einsatz eines Journals zur Nachverfolgung kürzlicher Metadatenänderungen reduziert sich die Dateisystemüberprüfung sogar für große Dateisysteme auf wenige Sekunden.

JFS

JFS, das „Journaling File System" wurde von IBM für AIX entwickelt. Die erste Betaversion des JFS-Linux-Ports erreichte die Linux-Gemeinde im Sommer 2000. Version 1.0.0 wurde im Jahre 2001 herausgegeben. JFS ist auf die Bedürfnisse von Server-Umgebungen mit hohem Durchsatz zugeschnitten, da hierbei einzig die Performance zählt. Als volles 64-Bit-Dateisystem unterstützt JFS große Dateien und Partitionen (LFS oder (engl. *Large File Support*)), was ein weiterer Pluspunkt für den Einsatz in Server-Umgebungen ist.

Ein genauerer Blick auf JFS zeigt, warum dieses Dateisystem möglicherweise eine gute Wahl für Ihren Linux-Server darstellt:

Effizientes Journaling JFS folgt wie ReiserFS einem „metadata only"-Ansatz. Anstelle einer ausführlichen Überprüfung werden lediglich Metadatenänderungen überprüft, die durch kürzliche Dateisystemaktivitäten hervorgerufen wurden. Dies spart enorm viel Zeit bei der Wiederherstellung. Zeitgleiche Aktivitäten, die mehrere Protokolleinträge erfordern, können in einem Gruppen-Commit zusammengefasst werden, wobei der Leistungsverlust des Dateisystems durch mehrfachen Schreibvorgang stark verringert wird.

Effiziente Verzeichnisverwaltung JFS hält an unterschiedlichen Verzeichnisstrukturen fest. Bei kleinen Verzeichnissen erlaubt es die direkte Speicherung des Verzeichnisinhaltes in seinem Inode. Für größere Verzeichnisse werden B^+trees verwendet, welche die Verzeichnisverwaltung erheblich erleichtern.

Bessere Speichernutzung durch dynamische Vergabe der Inodes Unter Ext2 müssen Sie die Inode-Dichte (von Verwaltungsinformationen belegter Speicher) vorab angeben. Dadurch wird die maximale Anzahl von Dateien oder Verzeichnissen Ihres Dateisystems limitiert. JFS erspart Ihnen diese Überlegungen — es weist Inode-Speicher dynamisch zu und stellt ihn bei Nichtbedarf wieder zur Verfügung.

XFS

Ursprünglich als Dateisystem für ihr IRIX-Betriebssystem gedacht, startete SGI die Entwicklung von XFS bereits in den frühen 90ern. Mit XFS sollte ein hochperformantes 64-Bit Journaling File System geschaffen werden, das den extremen Herausforderungen der heutigen Zeit gewachsen ist. XFS ist gut geeignet für den Umgang mit großen Dateien und zeigt gute Leistungen auf High-end-Hardware. Jedoch weist sogar XFS eine Schwäche auf. Wie ReiserFS, legt XFS großen Wert auf Metadatenintegrität und weniger auf Datenintegrität.

Ein kurzer Blick auf die Schlüsselfunktionen von XFS erklärt, warum es sich möglicherweise als starke Konkurrenz zu anderen Journaling File Systemen in der High-end-Datenverarbeitung herausstellen könnte.

Hohe Skalierbarkeit durch den Einsatz von „Allocation groups“ Zum Erstellungszeitpunkt eines XFS-Dateisystems wird das dem Dateisystem zugrundeliegende Block-Device in acht oder mehr lineare Bereiche gleicher Größe unterteilt. Diese werden als „allocation groups“ bezeichnet. Jede Allocation group verwaltet Inodes und freien Speicher selbst. Allocation groups können praktisch als „Dateisysteme im Dateisystem“ betrachtet werden. Da Allocation groups relativ autonom sind, kann der Kernel gleichzeitig mehrere von ihnen adressieren. Hier liegt der Schlüssel zur hohen Skalierbarkeit von XFS. Das Konzept der autonomen Allocation groups kommt natürlicherweise den Anforderungen von Multiprozessorsystemen entgegen.

Hohe Performance durch effiziente Festplattenspeicherverwaltung Freier Speicher und Inodes werden von B^+ trees innerhalb der Allocation

groups verwaltet. Der Einsatz von B^+ trees trägt zu einem Großteil zur Leistung und Skalierbarkeit von XFS bei. Ein wahrhaft einzigartiges Funktionsmerkmal von XFS ist die „delayed allocation". XFS verarbeitet die Speicherzuweisung (engl. *allocation*) durch Zweiteilung des Prozesses. Eine „schwebende" Transaktion wird in RAM gespeichert und der entsprechende Speicherplatz reserviert. XFS entscheidet noch nicht, wo genau (d.h. in welchen Dateisystemblöcken) die Daten gespeichert werden. Diese Entscheidung wird bis zum letztmöglichen Moment hinausgezögert. Einige kurzlebige, temporäre Daten werden somit niemals auf Platte gespeichert, da sie zum Zeitpunkt der Entscheidung über ihren Speicherort durch XFS bereits obsolet sind. So XFS erhöht die Leistung und verringert die Dateisystemfragmentation. Da allerdings eine verzögerte Zuordnung weniger Schreibvorgänge als in anderen Dateisystemen zur Folge hat, ist es wahrscheinlich, dass der Datenverlust nach einem Absturz während eines Schreibvorgangs größer ist.

Preallocation zur Vermeidung von Dateisystemfragmentation Vor dem Schreiben der Daten in das Dateisystem reserviert XFS den benötigten Speicherplatz für eine Datei (engl. *to preallocate*). Somit wird die Dateisystemfragmentation erhblich reduziert. Die Leistung wird erhöht, da die Dateiinhalte nicht über das gesamte Dateisystem verteilt werden.

Benutzerdefinierte Metadaten — „Extended Attributes" XFS bietet eine nette Funktion namens „extended attributes", welche MacOS-Benutzer an die „resource forks" auf ihren Systemen erinnern wird. Die Aktivierung der erweiterten Attribute in XFS ermöglicht die Verbindung beliebiger benutzerdefinierter Daten (bis zu 64 kB) mit einem Dateisystemobjekt. Diese Attribute werden nicht bei jedem Standarddateivorgang sichtbar, sondern mit speziellen, von bestimmten Applikationen verwendeten, Funktionsaufrufen. Erweiterte Attribute helfen bei der Unterscheidung zwischen den Dateidaten und den enthaltenen Metadaten, wie z.B. Kommentaren.

Weitere unterstützte Dateisysteme

Tabelle A.1 auf der nächsten Seite enthält weitere, von Linux unterstützte Dateisysteme. Sie werden hauptsächlich unterstützt, um die Kompatibilität und den Datenaustausch zwischen unterschiedlichen Medien oder fremden Betriebssystemen sicherzustellen.

`cramfs`	*Compressed ROM file system*: ein komprimiertes Dateisystem mit Lesezugriff für ROMs.
`hpfs`	*High Performance File System*: das IBM OS/2-Standarddateisystem — nur im Lesezugriffsmodus unterstützt.
`iso9660`	Standarddateisystem auf CD-ROMs.
`minix`	Dieses Dateisystem stammt aus akademischen Projekten zu Betriebssystemen und war das erste unter Linux genutzte Dateisystem. Heutzutage wird es als Dateisystem für Disketten verwendet.
`msdos`	*fat*, ursprünglich unter DOS verwendetes Dateisystem, das heute von verschiedenen Betriebssystemen genutzt wird.
`ncpfs`	Dateisystem zum Mounten von Novell-Volumes übers Netzwerk.
`nfs`	*Network File System*: Hierbei können Daten auf jedem beliebigen Rechner innerhalb eines Netzwerks gespeichert werden und der Zugriff kann über Netzwerk gewährt werden.
`smbfs`	*Server Message Block*: verwendet von Produkten wie z.B. Windows für den Dateizugriff über ein Netzwerk.
`sysv`	verwendet unter SCO UNIX, Xenix und Coherent (kommerzielle UNIX-Systeme für PCs).
`ufs`	verwendet von BSD, SunOS und NeXTstep. Nur im *Lesezugriffs*-Modus unterstützt.
`umsdos`	*UNIX on MSDOS*: aufgesetzt auf einem normalen `fat`-Dateisystem. Erhält UNIX-Funktionalität (Rechte, Links, lange Dateinamen) durch die Erstellung spezieller Dateien.
`vfat`	*Virtual FAT*: Erweiterung des `fat`-Dateisystems (unterstützt lange Dateinamen).
`ntfs`	*Windows NT file system*, nur Lesezugriff.

Tabelle A.1: *Dateisystemarten unter Linux*

Large File Support unter Linux

Ursprünglich unterstützte Linux Dateien mit einer maximalen Größe von 2 GB. Dies war ausreichend, solange niemand versuchte, große Datenbanken unter Linux zu verwalten. Aufgrund zunehmender Bedeutung für die

Dateisystem	Max. Dateigröße	Max. Dateisystemgröße
Ext2 oder Ext3 (1 kB Blockgröße)	16448 MB (~16 GB)	2048 GB (2 TB)
Ext2 oder Ext3 (2 kB Blockgröße)	256 GB	8192 GB (8 TB)
Ext2 oder Ext3 (4 kB Blockgröße)	2048 GB (2 TB)	16384 GB (16 TB)
Ext2 oder Ext3 (8 kB Blockgröße) (Systeme mit Pages von 8 kB (wie Alpha))	65568 GB (~64 TB)	32768 GB (32 TB)
ReiserFS 3.5	4 GB	16384 GB (16 TB)
ReiserFS 3.6 (unter Linux 2.4)	2^{60} Bytes (1 EB)	16384 GB (16 TB)
XFS	2^{63} Bytes (8 EB)	2048 GB (2 TB) (Linux Kernel Limit)
JFS (512 Bytes Blockgröße)	4194304 GB (4 PB)	512 TB
JFS (4 kB Blockgröße)	33554432 GB (32 PB)	4 PB

Tabelle A.2: *Maximale Größe von Dateisystemen*

Server-Datenverwaltung wurden Kernel und die GNU C Library zugunsten der Unterstützung von Dateien größer als 2 GB verändert. Es wurden neue Interfaces eingeführt, die von Applikationen genutzt werden können. Heutzutage bieten (fast) alle wichtigen Dateisysteme LFS-Unterstützung, welche High-End-Datenverarbeitung erlaubt.

Tabelle A.2 bietet einen Überblick über die derzeitigen Beschränkungen von Linux-Dateien und Dateisystemen für Kernel 2.4. Es bleibt zu wünschen, dass die unten genannten Zahlen mit dem Einzug künftiger Kernel-Versionen überholt sein werden und eine Unterstützung für noch größere Dateien und Dateisysteme möglich wird.

Weitere Informationen

Jedes der oben beschriebenen Dateisystemprojekte unterhält seine eigene Homepage, wo Sie Informationen aus Mailinglisten und weitere Dokumentation

sowie FAQs erhalten.

http://e2fsprogs.sourceforge.net/ext2.html
http://www.zipworld.com.au/~akpm/linux/ext3/
http://www.namesys.com/
http://oss.software.ibm.com/developerworks/opensource/jfs/
http://oss.sgi.com/projects/xfs/
Ein umfassendes mehrteiliges Tutorial zu Linux-Dateisystemen findet sich unter *IBM developerWorks*:
http://www-106.ibm.com/developerworks/library/l-fs.html

Einen Vergleich der verschiedenen Journaling File Systeme unter Linux befindet sich im Beitrag von Juan I. Santos Florido unter *Linuxgazette*: http://www.linuxgazette.com/issue55/florido.html.

Eine ausführliche Arbeit zu LFS unter Linux erhält man auf Andreas Jaegers LFS-Seiten: http://www.suse.de/~aj/linux_lfs.html.

Manual-Page von e2fsck

```
E2FSCK(8)                                                   E2FSCK(8)


NAME
       e2fsck - check a Linux second extended file system

SYNOPSIS
       e2fsck  [  -pacnyrdfvstFSV ] [ -b superblock ] [ -B block-
       size ] [ -l|-L bad_blocks_file ] [ -C fd ] [ -j  external-
       journal ] [ device

DESCRIPTION
       e2fsck  is used to check a Linux second extended file sys-
       tem (e2fs).  E2fsck also supports ext2  filesystems  coun-
       taining  a journal, which are also sometimes known as ext3
       filesystems.

       device is the special file  corresponding  to  the  device
              (e.g /dev/hdc1).

OPTIONS
       -a     This  option  does the same thing as the -p option.
              It is provided for backwards compatibility only; it
              is  suggested  that  people  use -p option whenever
              possible.

       -b superblock
              Instead of using  the  normal  superblock,  use  an
              alternative  superblock  specified  by  superblock.
              This option  is  normally  used  when  the  primary
              superblock has been corrupted.  The location of the
              backup superblock is dependent on the  filesystem's
              blocksize.   For  filesystems with 1k blocksizes, a
              backup superblock can be found at block  8193;  for
              filesystems with 2k blocksizes, at block 16384; and
              for 4k blocksizes, at block 32768.
```

Additional backup superblocks can be determined by using the mke2fs program using the -n option to print out where the superblocks were created. The -b option to mke2fs, which specifies blocksize of the filesystem must be specified in order for the superblock locations that are printed out to be accurate.

If an alternative superblock is specified and the filesystem is not opened read-only, e2fsck will make sure that the primary superblock is updated appropriately upon completion of the filesystem check.

-B blocksize
: Normally, e2fsck will search for the superblock at various different block sizes in an attempt to find the appropriate block size. This search can be fooled in some cases. This option forces e2fsck to only try locating the superblock at a particular blocksize. If the superblock is not found, e2fsck will terminate with a fatal error.

-c
: This option causes e2fsck to run the badblocks(8) program to find any blocks which are bad on the filesystem, and then marks them as bad by adding them to the bad block inode.

-C
: This option causes e2fsck to write completion information to the specified file descriptor so that the progress of the filesystem check can be monitored. This option is typically used by programs which are running e2fsck. If the file descriptor specified is 0, e2fsck will print a completion bar as it goes about its business. This requires that e2fsck is running on a video console or terminal.

-d
: Print debugging output (useless unless you are debugging e2fsck).

-f
: Force checking even if the file system seems clean.

-F
: Flush the filesystem device's buffer caches before beginning. Only really useful for doing e2fsck time trials.

-j external-journal
: Set the pathname where the external-journal for this filesystem can be found.

-l filename

```
              Add the blocks listed  in  the  file  specified  by
              filename  to the list of bad blocks.  The format of
              this file is the same as the one generated  by  the
              badblocks(8) program.

       -L filename
              Set  the  bad  blocks list to be the list of blocks
              specified by filename.  (This option is the same as
              the  -l  option,  except  the  bad  blocks  list is
              cleared before the blocks listed in  the  file  are
              added to the bad blocks list.)

       -n     Open the filesystem read-only, and assume an answer
              of 'no' to all questions.  Allows e2fsck to be used
              non-interactively.   (Note:  if  the  -c, -l, or -L
              options are specified in addition to the -n option,
              then  the  filesystem will be opened read-write, to
              permit the bad-blocks list to be updated.  However,
              no other changes will be made to the filesystem.)

       -p     Automatically  repair  ("preen")  the  file  system
              without any questions.

       -r     This option does nothing at  all;  it  is  provided
              only for backwards compatibility.

       -s     This  option  will byte-swap the filesystem so that
              it is using  the  normalized,  standard  byte-order
              (which  is i386 or little endian).  If the filesys-
              tem is already in the standard  byte-order,  e2fsck
              will take no action.

       -S     This  option will byte-swap the filesystem, regard-
              less of its current byte-order.

       -t     Print timing statistics for e2fsck.  If this option
              is  used  twice,  additional  timing statistics are
              printed on a pass by pass basis.

       -v     Verbose mode.

       -V     Print version information and exit.

       -y     Assume an answer of 'yes' to all questions;  allows
              e2fsck to be used non-interactively.

EXIT CODE
       The exit code returned by e2fsck is the sum of the follow-
       ing conditions:
            0    - No errors
            1    - File system errors corrected
            2    - File system errors corrected, system should
                   be rebooted if file system was mounted
```

```
       4    - File system errors left uncorrected
       8    - Operational error
       16   - Usage or syntax error
       128  - Shared library error


SIGNALS
       The following signals have the following effect when  sent
       to e2fsck.

       SIGUSR1
              This  signal  causes  e2fsck  to start displaying a
              completion bar.  (See discussion of the -C option.)
```

```
       SIGUSR2
              This signal causes e2fsck to stop displaying a com-
              pletion bar.

REPORTING BUGS
       Almost any piece of software will have bugs.  If you  man-
       age  to find a filesystem which causes e2fsck to crash, or
       which e2fsck is unable to repair, please report it to  the
       author.

       Please include as much information as possible in your bug
       report.  Ideally, include a  complete  transcript  of  the
       e2fsck  run,  so I can see exactly what error messages are
       displayed.  If you have a writeable filesystem  where  the
       transcript can be stored, the script(1) program is a handy
       way to save the output of e2fsck to a file.

       It is also useful to send the output of dumpe2fs(8).  If a
       specific  inode  or inodes seems to be giving e2fsck trou-
       ble, try running the debugfs(8) command and send the  out-
       put  of the stat(1u) command run on the relevant inode(s).
       If the inode is a directory, the debugfs dump command will
       allow  you to extract the contents of the directory inode,
       which can sent to me after being first run  through  uuen
       code(1).

       Always  include  the full version string which e2fsck dis-
       plays when it is run, so I know which version you are run-
       ning.


AUTHOR
       This  version  of  e2fsck  was  written  by  Theodore Ts’o
       <tytso@mit.edu>.

SEE ALSO
       mke2fs(8), tune2fs(8), dumpe2fs(8), debugfs(8)


E2fsprogs version 1.25    September 2001              E2FSCK(8)
```

Deutsche Übersetzung der GNU General Public License

Der folgende Text folgt im Wesentlichen der inoffiziellen Übersetzung von Katja Lachmann und der Überarbeitung von Peter Gerwinski (31. Oktober 1996, 4. Juni 2000).

Diese Übersetzung wird mit der Absicht angeboten, das Verständnis der *GNU General Public License* (GNU-GPL) zu erleichtern. Es handelt sich jedoch nicht um eine offizielle oder im rechtlichen Sinne anerkannte Übersetzung.

Die *Free Software Foundation* (FSF) ist nicht der Herausgeber dieser Übersetzung, und sie hat diese Übersetzung auch nicht als rechtskräftigen Ersatz für die Original-GNU-GPL (siehe `http://www.gnu.org/copyleft/gpl.html`) anerkannt. Da die Übersetzung nicht sorgfältig von Anwälten überprüft wurde, können die Übersetzer nicht garantieren, dass die Übersetzung die rechtlichen Aussagen der GNU-GPL exakt wiedergibt. Wenn Sie sichergehen wollen, dass von Ihnen geplante Aktivitäten im Sinne der GNU-GPL gestattet sind, halten Sie sich bitte an die englischsprachige Originalversion.

Die *Free Software Foundation* möchte Sie darum bitten, diese Übersetzung nicht als offizielle Lizenzbedingungen für von Ihnen geschriebene Programme zu verwenden. Bitte benutzen Sie hierfür stattdessen die von der *Free Software Foundation* herausgegebene englischsprachige Originalversion.

This is a translation of the GNU General Public License into German. This translation is distributed in the hope that it will facilitate understanding, but it is not an official or legally approved translation.

The Free Software Foundation is not the publisher of this translation and has not approved it as a legal substitute for the authentic GNU General Public License. The translation has not been reviewed carefully by lawyers, and therefore the translator

cannot be sure that it exactly represents the legal meaning of the GNU General Public License. If you wish to be sure whether your planned activities are permitted by the GNU General Public License, please refer to the authentic English version.

The Free Software Foundation strongly urges you not to use this translation as the official distribution terms for your programs; instead, please use the authentic English version published by the Free Software Foundation.

GNU General Public License

Deutsche Übersetzung der Version 2, Juni 1991

59 Temple Place, Suite 330, Boston, MA 02111-1307, USA

Diese Übersetzung ist kein rechtskräftiger Ersatz für die englischsprachige Originalversion!

Vorwort

Die meisten Softwarelizenzen sind daraufhin entworfen worden, Ihnen die Freiheit zu nehmen, die Software weiterzugeben und zu verändern. Im Gegensatz dazu soll Ihnen die *GNU General Public License*, die Allgemeine Öffentliche GNU-Lizenz, ebendiese Freiheit garantieren. Sie soll sicherstellen, dass die Software für alle Benutzer frei ist. Diese Lizenz gilt für den Großteil der von der *Free Software Foundation* herausgegebenen Software und für alle anderen Programme, deren Autoren ihr Datenwerk dieser Lizenz unterstellt haben. Auch Sie können diese Möglichkeit der Lizenzierung für Ihre Programme anwenden. (Ein anderer Teil der Software der *Free Software Foundation* unterliegt stattdessen der *GNU Library General Public License*, der Allgemeinen Öffentlichen GNU-Lizenz für Bibliotheken.)[1]

Die Bezeichnung *„freie" Software* bezieht sich auf Freiheit, nicht auf den Preis. Unsere Lizenzen sollen Ihnen die Freiheit garantieren, Kopien freier Software zu verbreiten (und etwas für diesen Service zu berechnen, wenn Sie möchten), die Möglichkeit, die Software im Quelltext zu erhalten oder den Quelltext auf Wunsch zu bekommen. Die Lizenzen sollen garantieren, dass Sie die Software ändern oder Teile davon in neuen freien Programmen verwenden dürfen – und dass Sie wissen, dass Sie dies alles tun dürfen.

[1] Mittlerweile wurde die GNU Library Public License von der GNU Lesser Public License abgelöst.

Um Ihre Rechte zu schützen, müssen wir Einschränkungen machen, die es jedem verbieten, Ihnen diese Rechte zu verweigern oder Sie aufzufordern, auf diese Rechte zu verzichten. Aus diesen Einschränkungen folgen bestimmte Verantwortlichkeiten für Sie, wenn Sie Kopien der Software verbreiten oder sie verändern.

Beispielsweise müssen Sie den Empfängern alle Rechte gewähren, die Sie selbst haben, wenn Sie – kostenlos oder gegen Bezahlung – Kopien eines solchen Programms verbreiten. Sie müssen sicherstellen, dass auch die Empfänger den Quelltext erhalten bzw. erhalten können. Und Sie müssen ihnen diese Bedingungen zeigen, damit sie ihre Rechte kennen.

Wir schützen Ihre Rechte in zwei Schritten: (1) Wir stellen die Software unter ein Urheberrecht (Copyright), und (2) wir bieten Ihnen diese Lizenz an, die Ihnen das Recht gibt, die Software zu vervielfältigen, zu verbreiten und/oder zu verändern.

Um die Autoren und uns zu schützen, wollen wir darüberhinaus sicherstellen, dass jeder erfährt, dass für diese freie Software keinerlei Garantie besteht. Wenn die Software von jemand anderem modifiziert und weitergegeben wird, möchten wir, dass die Empfänger wissen, dass sie nicht das Original erhalten haben, damit irgendwelche von anderen verursachte Probleme nicht den Ruf des ursprünglichen Autors schädigen.

Schließlich und endlich ist jedes freie Programm permanent durch Software-Patente bedroht. Wir möchten die Gefahr ausschließen, dass Distributoren eines freien Programms individuell Patente lizenzieren – mit dem Ergebnis, dass das Programm proprietär würde. Um dies zu verhindern, haben wir klargestellt, dass jedes Patent entweder für freie Benutzung durch jedermann lizenziert werden muss oder überhaupt nicht lizenziert werden darf.

Es folgen die genauen Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung:

Allgemeine Öffentliche GNU-Lizenz

Bedingungen für die Vervielfältigung, Verbreitung und Bearbeitung

0. Diese Lizenz gilt für jedes Programm und jedes andere Datenwerk, in dem ein entsprechender Vermerk des Copyright-Inhabers darauf hinweist, dass das Datenwerk unter den Bestimmungen dieser *General Public License* verbreitet werden darf. Im Folgenden wird jedes derartige Programm oder Datenwerk als „das Programm" bezeichnet; die Formulierung „auf dem Programm basierendes Datenwerk" bezeichnet das Programm sowie jegliche Bearbeitung des Programms im urheberrechtlichen Sinne, also ein Datenwerk, welches das Programm, auch auszugsweise, sei es unverändert oder verändert und/oder in eine andere Sprache übersetzt, enthält. (Im Folgenden wird

die Übersetzung ohne Einschränkung als „Bearbeitung“ eingestuft.) Jeder Lizenznehmer wird im Folgenden als „Sie“ angesprochen.

Andere Handlungen als Vervielfältigung, Verbreitung und Bearbeitung werden von dieser Lizenz nicht berührt; sie fallen nicht in ihren Anwendungsbereich. Der Vorgang der Ausführung des Programms wird nicht eingeschränkt, und die Ausgaben des Programms unterliegen dieser Lizenz nur, wenn der Inhalt ein auf dem Programm basierendes Datenwerk darstellt (unabhängig davon, dass die Ausgabe durch die Ausführung des Programmes erfolgte). Ob dies zutrifft, hängt von den Funktionen des Programms ab.

1. Sie dürfen auf beliebigen Medien unveränderte Kopien des Quelltextes des Programms, wie sie ihn erhalten haben, anfertigen und verbreiten. Voraussetzung hierfür ist, dass Sie mit jeder Kopie einen entsprechenden Copyright-Vermerk sowie einen Haftungsausschluss veröffentlichen, alle Vermerke, die sich auf diese Lizenz und das Fehlen einer Garantie beziehen, unverändert lassen und desweiteren allen anderen Empfängern des Programms zusammen mit dem Programm eine Kopie dieser Lizenz zukommen lassen.

Sie dürfen für den eigentlichen Kopiervorgang eine Gebühr verlangen. Wenn Sie es wünschen, dürfen Sie auch gegen Entgelt eine Garantie für das Programm anbieten.

2. Sie dürfen Ihre Kopie(n) des Programms oder einen Teil davon verändern, wodurch ein auf dem Programm basierendes Datenwerk entsteht; Sie dürfen derartige Bearbeitungen unter den Bestimmungen von Paragraph 1 vervielfältigen und verbreiten, vorausgesetzt, dass zusätzlich alle im Folgenden genannten Bedingungen erfüllt werden:

a) Sie müssen die veränderten Dateien mit einem auffälligen Vermerk versehen, der auf die von Ihnen vorgenommene Modifizierung und das Datum jeder Änderung hinweist.

b) Sie müssen dafür sorgen, dass jede von Ihnen verbreitete oder veröffentlichte Arbeit, die ganz oder teilweise von dem Programm oder Teilen davon abgeleitet ist, Dritten gegenüber als Ganzes unter den Bedingungen dieser Lizenz ohne Lizenzgebühren zur Verfügung gestellt wird.

c) Wenn das veränderte Programm normalerweise bei der Ausführung interaktiv Kommandos einliest, müssen Sie dafür sorgen, dass es, wenn es auf dem üblichsten Wege für solche interaktive Nutzung gestartet wird, eine Meldung ausgibt oder ausdruckt, die einen geeigneten

Copyright-Vermerk enthält sowie einen Hinweis, dass es keine Gewährleistung gibt (oder anderenfalls, dass Sie Garantie leisten), und dass die Benutzer das Programm unter diesen Bedingungen weiter verbreiten dürfen. Auch muss der Benutzer darauf hingewiesen werden, wie er eine Kopie dieser Lizenz ansehen kann. (Ausnahme: Wenn das Programm selbst interaktiv arbeitet, aber normalerweise keine derartige Meldung ausgibt, muss Ihr auf dem Programm basierendes Datenwerk auch keine solche Meldung ausgeben.)

Diese Anforderungen gelten für das bearbeitete Datenwerk als Ganzes. Wenn identifizierbare Teile des Datenwerkes nicht von dem Programm abgeleitet sind und vernünftigerweise als unabhängige und eigenständige Datenwerke für sich selbst zu betrachten sind, dann gelten diese Lizenz und ihre Bedingungen nicht für die betroffenen Teile, wenn Sie diese als eigenständige Datenwerke weitergeben. Wenn Sie jedoch dieselben Abschnitte als Teil eines Ganzen weitergeben, das ein auf dem Programm basierendes Datenwerk darstellt, dann muss die Weitergabe des Ganzen nach den Bedingungen dieser Lizenz erfolgen, deren Bedingungen für weitere Lizenznehmer somit auf das gesamte Ganze ausgedehnt werden – und somit auf jeden einzelnen Teil, unabhängig vom jeweiligen Autor.

Somit ist es nicht die Absicht dieses Abschnittes, Rechte für Datenwerke in Anspruch zu nehmen oder Ihnen die Rechte für Datenwerke streitig zu machen, die komplett von Ihnen geschrieben wurden; vielmehr ist es die Absicht, die Rechte zur Kontrolle der Verbreitung von Datenwerken, die auf dem Programm basieren oder unter seiner auszugsweisen Verwendung zusammengestellt worden sind, auszuüben.

Ferner bringt auch das einfache Zusammenlegen eines anderen Datenwerkes, das nicht auf dem Programm basiert, mit dem Programm oder einem auf dem Programm basierenden Datenwerk auf ein- und demselben Speicher- oder Vertriebsmedium dieses andere Datenwerk nicht in den Anwendungsbereich dieser Lizenz.

3. Sie dürfen das Programm (oder ein darauf basierendes Datenwerk gemäß Paragraph 2) als Objectcode oder in ausführbarer Form unter den Bedingungen der Paragraphen 1 und 2 kopieren und weitergeben – vorausgesetzt, dass Sie außerdem eine der folgenden Leistungen erbringen:

a) Liefern Sie das Programm zusammen mit dem vollständigen zugehörigen maschinenlesbaren Quelltext auf einem für den Datenaustausch üblichen Medium aus, wobei die Verteilung unter den Bedingungen der Paragraphen 1 und 2 erfolgen muss. Oder:

b) Liefern Sie das Programm zusammen mit einem mindestens drei Jahre lang gültigen schriftlichen Angebot aus, jedem Dritten eine vollständige maschinenlesbare Kopie des Quelltextes zur Verfügung zu stellen – zu nicht höheren Kosten als denen, die durch den physikalischen Kopiervorgang anfallen –, wobei der Quelltext unter den Bedingungen der Paragraphen 1 und 2 auf einem für den Datenaustausch üblichen Medium weitergegeben wird. Oder:

c) Liefern Sie das Programm zusammen mit dem schriftlichen Angebot der Zurverfügungstellung des Quelltextes aus, das Sie selbst erhalten haben. (Diese Alternative ist nur für nicht-kommerzielle Verbreitung zulässig und nur, wenn Sie das Programm als Objectcode oder in ausführbarer Form mit einem entsprechenden Angebot gemäß Absatz b erhalten haben.)

Unter dem Quelltext eines Datenwerkes wird diejenige Form des Datenwerkes verstanden, die für Bearbeitungen vorzugsweise verwendet wird. Für ein ausführbares Programm bedeutet „der komplette Quelltext": Der Quelltext aller im Programm enthaltenen Module einschließlich aller zugehörigen Modulschnittstellen-Definitionsdateien sowie der zur Kompilation und Installation verwendeten Skripte. Als besondere Ausnahme jedoch braucht der verteilte Quelltext nichts von dem zu enthalten, was üblicherweise (entweder als Quelltext oder in binärer Form) zusammen mit den Hauptkomponenten des Betriebssystems (Kernel, Compiler usw.) geliefert wird, unter dem das Programm läuft – es sei denn, diese Komponente selbst gehört zum ausführbaren Programm.

Wenn die Verbreitung eines ausführbaren Programms oder von Objectcode dadurch erfolgt, dass der Kopierzugriff auf eine dafür vorgesehene Stelle gewährt wird, so gilt die Gewährung eines gleichwertigen Zugriffs auf den Quelltext als Verbreitung des Quelltextes, auch wenn Dritte nicht dazu gezwungen sind, den Quelltext zusammen mit dem Objectcode zu kopieren.

4. Sie dürfen das Programm nicht vervielfältigen, verändern, weiter lizenzieren oder verbreiten, sofern es nicht durch diese Lizenz ausdrücklich gestattet ist. Jeder anderweitige Versuch der Vervielfältigung, Modifizierung, Weiterlizenzierung und Verbreitung ist nichtig und beendet automatisch Ihre Rechte unter dieser Lizenz. Jedoch werden die Lizenzen Dritter, die von Ihnen Kopien oder Rechte unter dieser Lizenz erhalten haben, nicht beendet, solange diese die Lizenz voll anerkennen und befolgen.

5. Sie sind nicht verpflichtet, diese Lizenz anzunehmen, da Sie sie nicht unterzeichnet haben. Jedoch gibt Ihnen nichts anderes die Erlaubnis, das Programm oder von ihm abgeleitete Datenwerke zu verändern oder zu verbreiten. Diese Handlungen sind gesetzlich verboten, wenn Sie diese Lizenz nicht anerkennen. Indem Sie das Programm (oder ein darauf basierendes Datenwerk) verändern oder verbreiten, erklären Sie Ihr Einverständnis mit dieser Lizenz und mit allen ihren Bedingungen bezüglich der Vervielfältigung, Verbreitung und Veränderung des Programms oder eines darauf basierenden Datenwerks.

6. Jedes Mal, wenn Sie das Programm (oder ein auf dem Programm basierendes Datenwerk) weitergeben, erhält der Empfänger automatisch vom ursprünglichen Lizenzgeber die Lizenz, das Programm entsprechend den hier festgelegten Bestimmungen zu vervielfältigen, zu verbreiten und zu verändern. Sie dürfen keine weiteren Einschränkungen der Durchsetzung der hierin zugestandenen Rechte des Empfängers vornehmen. Sie sind nicht dafür verantwortlich, die Einhaltung dieser Lizenz durch Dritte durchzusetzen.

7. Sollten Ihnen infolge eines Gerichtsurteils, des Vorwurfs einer Patentverletzung oder aus einem anderen Grunde (nicht auf Patentfragen begrenzt) Bedingungen (durch Gerichtsbeschluss, Vergleich oder anderweitig) auferlegt werden, die den Bedingungen dieser Lizenz widersprechen, so befreien Sie diese Umstände nicht von den Bestimmungen dieser Lizenz. Wenn es Ihnen nicht möglich ist, das Programm unter gleichzeitiger Beachtung der Bedingungen in dieser Lizenz und Ihrer anderweitigen Verpflichtungen zu verbreiten, dann dürfen Sie als Folge das Programm überhaupt nicht verbreiten. Wenn zum Beispiel ein Patent nicht die gebührenfreie Weiterverbreitung des Programms durch diejenigen erlaubt, die das Programm direkt oder indirekt von Ihnen erhalten haben, dann besteht der einzige Weg, sowohl das Patentrecht als auch diese Lizenz zu befolgen, darin, ganz auf die Verbreitung des Programms zu verzichten.

Sollte sich ein Teil dieses Paragraphen als ungültig oder unter bestimmten Umständen nicht durchsetzbar erweisen, so soll dieser Paragraph seinem Sinne nach angewandt werden; im übrigen soll dieser Paragraph als Ganzes gelten.

Zweck dieses Paragraphen ist nicht, Sie dazu zu bringen, irgendwelche Patente oder andere Eigentumsansprüche zu verletzen oder die Gültigkeit solcher Ansprüche zu bestreiten; dieser Paragraph hat einzig den Zweck, die Integrität des Verbreitungssystems der freien Software zu schützen, das durch die Praxis öffentlicher Lizenzen verwirklicht wird. Viele Leute haben großzügige Beiträge zu dem großen Angebot der mit diesem System verbreiteten

Software im Vertrauen auf die konsistente Anwendung dieses Systems geleistet; es liegt am Autor/Geber, zu entscheiden, ob er die Software mittels irgendeines anderen Systems verbreiten will; ein Lizenznehmer hat auf diese Entscheidung keinen Einfluss.

Dieser Paragraph ist dazu gedacht, deutlich klarzustellen, was als Konsequenz aus dem Rest dieser Lizenz betrachtet wird.

8. Wenn die Verbreitung und/oder die Benutzung des Programms in bestimmten Staaten entweder durch Patente oder durch urheberrechtlich geschützte Schnittstellen eingeschränkt ist, kann der Urheberrechtsinhaber, der das Programm unter diese Lizenz gestellt hat, eine explizite geographische Begrenzung der Verbreitung angeben, in der diese Staaten ausgeschlossen werden, so dass die Verbreitung nur innerhalb und zwischen den Staaten erlaubt ist, die nicht ausgeschlossen sind. In einem solchen Fall beinhaltet diese Lizenz die Beschränkung, als wäre sie in diesem Text niedergeschrieben.

9. Die *Free Software Foundation* kann von Zeit zu Zeit überarbeitete und/oder neue Versionen der *General Public License* veröffentlichen. Solche neuen Versionen werden vom Grundprinzip her der gegenwärtigen entsprechen, können aber im Detail abweichen, um neuen Problemen und Anforderungen gerecht zu werden.

Jede Version dieser Lizenz hat eine eindeutige Versionsnummer. Wenn in einem Programm angegeben wird, dass es dieser Lizenz in einer bestimmten Versionsnummer oder „jeder späteren Version“ *("any later version")* unterliegt, so haben Sie die Wahl, entweder den Bestimmungen der genannten Version zu folgen oder denen jeder beliebigen späteren Version, die von der *Free Software Foundation* veröffentlicht wurde. Wenn das Programm keine Versionsnummer angibt, können Sie eine beliebige Version wählen, die je von der *Free Software Foundation* veröffentlicht wurde.

10. Wenn Sie den Wunsch haben, Teile des Programms in anderen freien Programmen zu verwenden, deren Bedingungen für die Verbreitung anders sind, schreiben Sie an den Autor, um ihn um die Erlaubnis zu bitten. Für Software, die unter dem Copyright der *Free Software Foundation* steht, schreiben Sie an die *Free Software Foundation*; wir machen zu diesem Zweck gelegentlich Ausnahmen. Unsere Entscheidung wird von den beiden Zielen geleitet werden, zum einen den freien Status aller von unserer freien Software abgeleiteten Datenwerke zu erhalten und zum anderen das gemeinschaftliche Nutzen und Wiederverwenden von Software im allgemeinen zu fördern.

Keine Gewährleistung

11. **Da das Programm ohne jegliche Kosten lizenziert wird, besteht keinerlei Gewährleistung für das Programm, soweit dies gesetzlich zulässig ist. Sofern nicht anderweitig schriftlich bestätigt, stellen die Copyright-Inhaber und/oder Dritte das Programm so zur Verfügung, „wie es ist“, ohne irgendeine Gewährleistung, weder ausdrücklich noch implizit, einschließlich – aber nicht begrenzt auf – Marktreife oder Verwendbarkeit für einen bestimmten Zweck. Das volle Risiko bezüglich Qualität und Leistungsfähigkeit des Programms liegt bei Ihnen. Sollte sich das Programm als fehlerhaft herausstellen, liegen die Kosten für notwendigen Service, Reparatur oder Korrektur bei Ihnen.**

12. **In keinem Fall, außer wenn durch geltendes Recht gefordert oder schriftlich zugesichert, ist irgendein Copyright-Inhaber oder irgendein Dritter, der das Programm wie oben erlaubt modifiziert oder verbreitet hat, Ihnen gegenüber für irgendwelche Schäden haftbar, einschließlich jeglicher allgemeiner oder spezieller Schäden, Schäden durch Seiteneffekte (Nebenwirkungen) oder Folgeschäden, die aus der Benutzung des Programms oder der Unbenutzbarkeit des Programms folgen (einschließlich – aber nicht beschränkt auf – Datenverluste, fehlerhafte Verarbeitung von Daten, Verluste, die von Ihnen oder anderen getragen werden müssen, oder dem Unvermögen des Programms, mit irgendeinem anderen Programm zusammenzuarbeiten), selbst wenn ein Copyright-Inhaber oder Dritter über die Möglichkeit solcher Schäden unterrichtet worden war.**

Ende der Bedingungen

Anhang: Wie Sie diese Bedingungen auf Ihre eigenen, neuen Programme anwenden können

Wenn Sie ein neues Programm entwickeln und wollen, dass es vom größtmöglichen Nutzen für die Allgemeinheit ist, dann erreichen Sie das am besten, indem Sie es zu freier Software machen, die jeder unter diesen Bestimmungen weiterverbreiten und verändern kann.

Um dies zu erreichen, fügen Sie die folgenden Vermerke zu Ihrem Programm hinzu. Am sichersten ist es, sie an den Anfang einer jeden Quelldatei zu stellen, um den Gewährleistungsausschluss möglichst deutlich darzustellen; zumindest aber sollte jede Datei eine Copyright-Zeile besitzen sowie einen kurzen Hinweis darauf, wo die vollständigen Vermerke zu finden sind.

> *eine Zeile mit dem Programmnamen und einer kurzen Beschreibung*
> Copyright (C) 19*yy* *Name des Autors*

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Auf Deutsch:

eine Zeile mit dem Programmnamen und einer kurzen Beschreibung
Copyright (C) 19*jj* *Name des Autors*

Dieses Programm ist freie Software. Sie können es unter den Bedingungen der GNU General Public License, wie von der Free Software Foundation veröffentlicht, weitergeben und/oder modifizieren, entweder gemäß Version 2 der Lizenz oder (nach Ihrer Option) jeder späteren Version.

Die Veröffentlichung dieses Programms erfolgt in der Hoffnung, dass es Ihnen von Nutzen sein wird, aber OHNE IRGENDEINE GARANTIE, sogar ohne die implizite Garantie der MARKTREIFE oder der VERWENDBARKEIT FÜR EINEN BESTIMMTEN ZWECK. Details finden Sie in der GNU General Public License.

Sie sollten eine Kopie der GNU General Public License zusammen mit diesem Programm erhalten haben. Falls nicht, schreiben Sie an die Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307, USA.

Fügen Sie auch einen kurzen Hinweis hinzu, wie Sie elektronisch und per Brief erreichbar sind.

Wenn Ihr Programm interaktiv ist, sorgen Sie dafür, dass es nach dem Start einen kurzen Vermerk ausgibt:

Gnomovision version 69, Copyright (C) 19*yy* *Name des Autors*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’. This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

Auf Deutsch:

> Gnomovision Version 69, Copyright (C) 19*jj* *Name des Autors*
> Für Gnomovision besteht KEINERLEI GARANTIE; geben Sie 'show w' für Details ein. Gnonovision ist freie Software, die Sie unter bestimmten Bedingungen weitergeben dürfen; geben Sie 'show c' für Details ein.

Die hypothetischen Kommandos `show w` und `show c` sollten die entsprechenden Teile der GNU-GPL anzeigen. Natürlich können die von Ihnen verwendeten Kommandos anders heißen als `show w` und `show c`; es könnten auch Mausklicks oder Menüpunkte sein – was immer am besten in Ihr Programm passt.

Soweit vorhanden, sollten Sie auch Ihren Arbeitgeber (wenn Sie als Programmierer arbeiten) oder Ihre Schule einen Copyright-Verzicht für das Programm unterschreiben lassen. Hier ein Beispiel. Die Namen müssen Sie natürlich ändern.

> Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.
> *Unterschrift von Ty Coon*, 1 April 1989
> Ty Coon, President of Vice

Auf Deutsch:

> Die Yoyodyne GmbH erhebt keinen urheberrechtlichen Anspruch auf das von James Hacker geschriebene Programm , Gnomovision' (einem Schrittmacher für Compiler).
> *Unterschrift von Ty Coon*, 1. April 1989
> Ty Coon, Vizepräsident

Diese *General Public License* gestattet nicht die Einbindung des Programms in proprietäre Programme. Ist Ihr Programm eine Funktionsbibliothek, so kann es sinnvoller sein, das Binden proprietärer Programme mit dieser Bibliothek zu gestatten. Wenn Sie dies tun wollen, sollten Sie die GNU Library General Public License anstelle dieser Lizenz verwenden.

Literaturverzeichnis

[Alm96] ALMESBERGER, Werner: *LILO User's guide*, 1996. – (siehe Datei `/usr/share/doc/lilo/user.dvi`)

[Bai97] BAILEY, Edward C.: *Maximum RPM*. Red Hat, 1997. – (ISBN 1-888172-78-9)

[BBD+97] BECK, Michael; BÖHME, Harald; DZIADZKA, Mirko; KUNITZ, Ulrich; MAGNUS, Robert ; VERWORNER, Dirk: *Linux-Kernel-Programmierung*. 4. Aufl. Addison Wesley GmbH, 1997. – (ISBN 3-8273-1144-6)

[BD98] BORKNER-DELCARLO, Olaf: *Linux im kommerziellen Einsatz*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19465-7)

[BD99] BORKNER-DELCARLO, Olaf: *Das Samba-Buch*. SuSE PRESS, 1999. – (ISBN 3-930419-93-9)

[CAR93] COSTALES, Bryan; ALLMAN, Eric ; RICKERT, Neil: *sendmail*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-056-2)

[CB96] CHESWICK, William R.; BELLOVIN, Steven M.: *Firewalls und Sicherheit im Internet*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-875-x)

[CZ96] CHAPMAN, Brent; ZWICKY, Elisabeth D.: *Einrichten von Internet Firewalls. Sicherheit im Internet gewährleisten.*. O'Reilly & Associates, Inc., 1996. – (ISBN 3-930673312)

[DR99] DAWSON, Terry; RUBINI, Alessandro: *NET3-4 HOWTO*, v1.5, August 1999. – (siehe Datei `/usr/share/doc/howto/en/NET3-4-HOWTO.gz`)

[EH98] ECKEL, George; HARE, Chris: *Linux – Internet Server*. Carl Hanser Verlag, 1998. – (ISBN 3-446-19044-9)

[FCR93] FANG, Chin; CROSSON, Bob ; RAYMOND, Eric S.: *The Hitchhiker's Guide to X386/XFree86 Video Timing (or, Tweaking your Monitor for Fun and Profit)*, 1993. – (siehe Datei `/usr/X11/lib/X11/doc/VideoModes.doc`)

[Fis00] FISCHER, Thorsten: *GUI-Programmierung mit GTK+ (Handbuch und Referenz)*. SuSE PRESS, 2000. – ISBN (3–934678–42–4)

[Fri93] FRISCH, Æleen: *Essential System Administration*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-80-3)

[Gil92] GILLY, Daniel: *UNIX in a nutshell: System V Edition*. O'Reilly & Associates, Inc., 1992. – (ISBN 1-56592-001-5)

[GMR97] GOOSSENS, Michel; MITTELBACH, Frank ; RAHTZ, Sebastian: *The LaTeX Graphics Companion*. Addison Wesley Longman, 1997. – (ISBN 0-201-85469-4)

[GMS94] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *The LaTeX Companion*. Addison Wesley GmbH, 1994. – (ISBN 0-201-54199-8)

[GMS96] GOOSSENS, Michel; MITTELBACH, Frank ; SAMARIN, Alexander: *Der LaTeX-Begleiter*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-646-3)

[GR99] GOOSSENS, Michel; RAHTZ, Sebastian: *The LaTeX Web Companion*. Addison Wesley Longman, 1999. – (ISBN 0-201-43322-7)

[GS93] GARFINKEL, Simson; SPAFFORD, Gene: *Practical UNIX Security*. O'Reilly & Associates, Inc., 1993. – (ISBN 0-937175-72-2)

[Hei96] HEIN, Jochen: *Linux-Companion zur Systemadministration*. Addison Wesley GmbH, 1996. – (ISBN 3-89319-869-5)

[Her92] HEROLD, H.: *UNIX Grundlagen*. Addison Wesley GmbH, 1992. – (ISBN 3-89319-542-8)

[HHMK96] HETZE, Sebastian; HOHNDEL, Dirk; MÜLLER, Martin ; KIRCH, Olaf: *Linux Anwenderhandbuch*. 6. Aufl. LunetIX Softfair, 1996. – (ISBN 3-929764-05-9)

[Hof97] HOFFMANN, Erwin: EMail-Gateway mit qmail. In: *iX* 12 (1997), S. 108ff.

[HR98] HÖLZER, Matthias; RÖHRIG, Bernhard: *KDE – Das K Desktop Environment*. Computer & Literatur, 1998. – (ISBN 3-932311-50-7)

[Hun95] HUNT, Craig: *TCP/IP Netzwerk Administration*. O'Reilly & Associates, Inc., 1995. – (ISBN 3-930673-02-9)

[JT98] JOHNSON, Michael K.; TROAN, Erik W.: *Anwendungen entwickeln unter Linux*. Addison Wesley GmbH, 1998. – (ISBN 3-8273-1449-6)

[Kie95] KIENLE, Micheal: TIS: Toolkit für anwendungsorientierte Firewall-Systeme. In: *iX* 8 (1995), S. 140ff.

[Kir95] KIRCH, Olaf: *LINUX Network Administrator's Guide*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-087-2)

[Kof99] KOFLER, Michael: *Linux – Installation, Konfiguration, Anwendung*. 4. Aufl. Addison Wesley GmbH, 1999. – (ISBN 3-8273-1475-5)

[Kop94] KOPKA, Helmut: *LaTeX-Einführung*. Addison Wesley GmbH, 1994. – (ISBN 3-89319-664-1)

[Kopff] KOPKA, Helmut: *LaTeX*. Addison Wesley GmbH, 1996 ff. – 3 Bde. (ISBN 3-8273-1025-3; 3-8273-1229-9; 3-89319-666-8)

[Kun95] KUNITZ, Ulrich: Sicherheit fast kostenlos: Einrichtung eines kostenlosen Firewall-Systems. In: *iX* 9 (1995), S. 176ff.

[Lam90] LAMB, Linda: *Learning the vi Editor*. O'Reilly & Associates, Inc., 1990. – (ISBN 0-937175-67-6)

[Lef96] LEFFLER, Sam: *HylaFAX Home Page*, 1996

[Meg98] MEGGINSON, David: *Structuring XML Documents*. Prentice-Hall, 1998. – ISBN (0–13–642299–3)

[Moh98] MOHR, James: *UNIX-Windows-Integration*. International Thomson Publishing, 1998. – (ISBN 3-8266-4032-2)

[OT92] O'REILLY, Tim; TODINO, Grace: *Managing UUCP and Usenet*. O'Reilly & Associates, Inc., 1992. – (ISBN 0-937175-93-5)

[POL97] PEEK, Jerry; O'REILLY, Tim ; LOUKIDES, Mike: *Unix Power Tools*. 2. Aufl. Sebastopol : O'Reilly & Associates, Inc., 1997

[Rub98] RUBINI, Alessandro: *Linux-Gerätetreiber*. O'Reilly & Associates, Inc., 1998. – (ISBN 3-89721-122-X)

[Sch98] SCHEIDERER, Jürgen: Sicherheit Kostenlos - Firewall mit Linux. In: *iX* 12 (1998)

[Sto98] STOLL, Clifford: *Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer-TB.-Vlg., 1998. – (ISBN 3596139848)

[SuS02a] *SuSE Linux. Basis*. 1. Nürnberg : SuSE Linux AG, 2002

[SuS02b] *SuSE Linux. Benutzerhandbuch*. 1. Nürnberg : SuSE Linux AG, 2002

[SuS02c] *SuSE Linux. Die Programme*. 1. Nürnberg : SuSE Linux AG, 2002

[The96] THE XFREE86™-TEAM: *XF86Config(4/5) – Configuration File for Xfree86™*, 1996. – Manual-Page zu XFree86™

[TSP93] TODINO, Grace; STRANG, John ; PEEK, Jerry: *Learning the UNIX operating system*. O'Reilly & Associates, Inc., 1993. – (ISBN 1-56592-060-0)

[Wel94] WELSH, Matt: *Linux Installation and Getting Started*. 2. Aufl. SuSE GmbH, 1994. – (ISBN 3-930419-03-3)

[WK95] WELSH, Matt; KAUFMAN, Lars: *Running Linux*. O'Reilly & Associates, Inc., 1995. – (ISBN 1-56592-100-3)

[WK98] WELSH, Matt; KAUFMAN, Lars: *Linux – Wegweiser zur Installation & Konfiguration*. 2. Aufl. O'Reilly & Associates, Inc., 1998. – (ISBN 3-930673-58-4)

[WM99] WALSH, Norman; MUELLNER, Leonard: *DocBook. The Definiteve Guide*. O'Reilly & Associates, Inc., 1999. – ISBN (1–56592–580–7)

Index

Symbole

/etc/conf.modules .... *siehe* /etc/modules.conf
/etc/hosts 262
/etc/init.d/boot 46
/etc/inittab 226
/etc/lilo.conf 92, 93
/etc/logfiles .... *siehe* Protokoll-Dateien
/etc/modules.conf 191
/etc/profile ..... *siehe* bash, /etc/profile
/etc/resolv.conf 43, 202
xdm 245

A

ACPI 171
Adressen
- IP 274
- MAC 274
Advanced Powermanagement 257
AMaViS 237
Apache
- mod_php4 44
- Squid 363
APM 171
- Kernelparameter 45
Apple
- Netatalk 332
ATA-RAID-Controller ...... *siehe* Hardware, Promise-Controller
ATAPI-CD-ROM hängt 24
Authentifizierung 40
autoexec.bat 110
autoexec.bat 231
autofs 240
- Dateien über NIS 46

B

bash
- /etc/profile 197
Befehl
- ulimit 200
Benutzer anlegen
- Schwierigkeiten 294
Benutzernamen
- Änderung 47
Bildschirm .... *siehe* SuSE-Bildschirm, deaktivieren
Bildschirmeinrichtung 70
BIND 297
- BIND8 300
- BIND9 300
BIOS
- Virus Protection 16
Bootbildschirm 99
Bootdisk 20
- installieren mit 9
Bootdiskette 45, 88, 91
- Erzeugen mit dd 22
- Erzeugen mit rawrite 21
Booten 225, 381
- Ablauf 86
- Bootmanager 88
- GRUB 107–110
- initial ramdisk 202
- Konzept 225
- Konzepte 87
- LILO 85
- Methoden 15
- Rechner bleibt hängen .. *siehe* BIOS, Virus Protection
- Startmechanismus mit loadlin ... 110

- von CD2 21
- von Diskette 20
- von Disketten 21
Bootgrafik 99
Bootkonzepte 87
Bootloader
- GRUB 107
- LILO 85
Bootmanager 85
- boot.sys 88
- LILO 88
- Windows NT 88
Bootmenü 110
Bootschwierigkeiten .. *siehe* Installation, Safe Settings
Bootsektor 86
Bootvorgang 86

C

CD-ROM-Laufwerk
- am Parallelport 24
- Unterstützung durch Linux 23
CD-ROM-Laufwerk
- hängt 24
CD-ROM-Laufwerk hängt 25
Check 381
command not found 262
Compose . *siehe* Tastaturbelegung, Compose
conf.modules .... *siehe* modules.conf
`conf.modules` .... *siehe* /etc/modules.conf
config.sys 110
configuration files
- squid.conf 363
Core-Dateien 200
Crash 381
cron 198, 243

D

Dateien
- groß 378–379
Dateien finden 46
Dateirechte 260
Dateisystem
- FHS 196
- TeX 196
Dateisysteme 371–380
- Auswahl 372
- Beschränkungen 379
- Ext2 372–373
- Ext3 373–374
- Intermezzo 248
- JFS 375–376
- ReiserFS 374–375
- Termini 371
- unterstützt 377–378
- XFS 376–377
DCF77 265
Deinstallation
- Linux 102
- Squid 353
DENIC 297
depmod 190
DHCP
- Clientkonfiguration 253
- Relay Agent 245
- Serverkonfiguration 244
Diskette
- Booten von 88
- Formatieren 22
DMA .... *siehe* IDE-DMA
- abschalten 246
- einschalten 246
DNS 277, 297
- Forwarding 298
- Logging 301
- Mail Exchanger 278
- NIC 278
- Optionen 300
- Problemanalyse 298
- Squid und 353
- Starten 297
- Timeout 44
- top level domain 277
- Zonedateien 303
- Zonen 301
DNS-Domain 310
DNS:umgekehrte Adress-Auflösung 305
DocBook .... *siehe* SGML, DocBook
Domain 289
Domain Name Service 297
DOS
- Booten 104
- Bootmenü 110
Drivespace 26
Drucken 69
Druckereinrichtung 69
DVB 246
Dynamische IP-Adresse 262

E

E-Mail 70
`2fsck` 381
EIDE
- Spezielle Chipsätze 43
Erstinstallation

- Bootdiskette unter unixartigem System erstellen 22
- Bootdisketten 21
- Booten von CD2 21
- Booten von Diskette 20
- künftige Boot-Methode 15
- linuxrc 9
- Startbildschirm 8
- Startmechanismus mit loadlin ... 110
exportieren 313

F

fdisk
- mbr 103
FHS .... *siehe* Dateisystem, FHS
Finden von Dateien 46
FireGL 9
Firewall 73
- Aktivieren 237
- Squid 360
Firewire 148
Framebuffer 241
`free` 201
FTP
- Anonymes FTP 41
FTP-Server
- einrichten 196
- Verzeichnis 47
Funkuhr 265

G

GDT RAID5-Controller .... *siehe* ICP Vortex
GNOME
- Übersetzen 49
GPL 387
Grafik
- 3D 236
Grafikkarte 70
Grafische Oberfläche 70
Grafischer Hintergrund .... *siehe* SuSE-Bildschirm, deaktivieren
group 310
GRUB 107
Gruppennamen
- Änderung 47

H

harden_suse 47
Hardware
- Drucker 260
- Hotplug 246
- Joystick 249
- Laptop 151
- Notebook 151
- Promise-Controller 35
Hintergrund
- grafischer .... *siehe* SuSE-Bildschirm, deaktivieren
Hochverfügbarkeit
- ArgoUPS 239
hosts 291
Hotplug 143, 286
- Firewire 148
- Kameras 146
- Mäuse 146
- Netzwerkgeräte 146
- PCI 147
- PCMCIA 147
- Speichergeräte 146
- Tastaturen 146
- unter Linux 144
- USB 145
HTTP-Server
- einrichten 197
- Verzeichnis 47
httpd 237

I

I18N 220
ICP Vortex-Controller
- Installation schlägt fehl 14
IDE-DMA 45
IDE-Festplatte
- ATA-RAID-Controller .... *siehe* Hardware, Promise-Controller
importieren 312
Info (`info`) 200
init 226
- Skripte 229
initial ramdisk 202
initrd 249
inittab 226
insmod 190
Installation
- Autoinstallation 240
- CD-ROM-Laufwerk am Parallelport . 25
- FTP 18
- GRUB 47
- LILO 47
- mailman 47
- majordomo 47
- mit YaST, textbasiert 8
- Netz als Quelle 18
- NFS 18
- Pakete deinstallieren 49

- Pakete installieren 49
- PCMCIA 161
- postfix 47
- Safe Settings 45
- sendmail 47
Intermezzo 248
IP-Adresse
- dynamisch 262
IP-Adressen 274
- IPv6 278
· Aufbau 280
· Netzmasken 282
· Präfixe 281
- Netzmasken 274
- Netzwerkklassen 274
- privat 277
IP-Forwarding 262
IPv6 44
IrDA 178
- Schnittstelle einstellen 248
ispell 248

J

Java 248

K

Kernel 185
- Compilierung 185
- Debugging 263
- Konfiguration 187
- Module 189
- separate Module 39
- Sysrq 263
Kernel Module
- Netzwerkkarten 284
Kernel Module Loader 191
Kernel too big 192
Kernel-Module
- Konfigurationsdatei 39
kerneld 191
Kerneldaemon 191
Kernelparameter
- realmode-power-off 45
Kmod 191
Konfiguration
- Ändern 233
- IPv6 287
- LILO 92
- manuell 287
- Netzzeit 265
- Squid 354
- YaST2 284
Konfigurationsdatei 235
Konfigurationsdateien 289
- exports 314
- host.conf 291, 292
- HOSTNAME 295
- ifroute-* 296
- menu.lst 108
- named.conf 299
- Netzwerk 291
- nscd.conf 294
- nsswitch.conf 292
- resolv.conf 289
- routes 296
- squid.conf 354, 360
- squidguard.conf 365
Konsole 241, 245
- virtuell 219

L

L10N 220
Löschen
- LILO 102
- Linux 102
LAN 284
Laptop 151
ldconfig 42
LILO 85
- Beispielkonfigurationen 104
- Bestandteile 90
- Deinstallation 100
- DOS/Win95 booten 104
- Entfernen 102
- Installation 100
- Konfiguration 92
- Probleme 106
- Windows 2000 booten 105
- Windows NT booten 105
- wohin installieren 91
Linux
- Deinstallieren 102
- Löschen 102
- Update 33
Linux Standard Base 196
linux.par 110
linuxrc 207
Lizenz 387
loadlin 110
- funktioniert nicht 26
- startet nicht 26
Local Area Network .... *siehe* LAN
locate 46, 250
Logdateien .... *siehe* Protokoll-Dateien
Logical Volume Manager .... *siehe* YaST2,Logical Volume Manager

Login 245
- Login-Shell 40
- PAM 40, 41
- remote 46
LSB .... *siehe* Linux Standard Base
- Pakete installieren 48
lsmod 190
LVM .... *siehe* YaST2,LVM

M

Mac OS 332
Mail
- Postfix 246
makewhatis 41
Manpages .... *siehe* Manual-Pages, *siehe* Manual-Pages
Manual-Pages 200
- Datenbank anlegen 244
- Index 41
Masquerading
- IP-Forwarding 262
Maus 252
- pine 46
MBR ...... 86, 92, *siehe* Master Boot Record
`mk_initrd` .... *siehe* mkinitrd
`mkinitrd` 206
mod_php4 44
modinfo 191
modprobe 190
Modul
- Übersetzen 192
- Laden 209
- Parameter 210
- Umgang 190
Module 189
`modules.conf` .... *siehe* /etc/modules.conf
mount 313
mountd 314
msdos.sys 110
Multi_key *siehe* Tastaturbelegung, Compose

N

Name Service Switch 292
Name Service Cache Daemon 294
Namensdienst 324
Nameserver 289, 297
- BIND 297
Netatalk 332
NetBIOS 324
Network File System .... *siehe* NFS
Network Information Service ..... *siehe* NIS
Netzwerk
- Broadcastadresse 276
- DHCP Relay 245
- DNS 277
- E-Mail 251
- Grundkonfiguration 252
- IP-Adressen 274
- Konfiguration 284
  · IPv6 287
- Konfiguration DHCP Server 244
- Konfigurationsdateien 289
- Localhost 276
- Monitorsoftware 240
- Netzwerkbasisadresse 276
- Netzwerkkarte konfigurieren 255
- NFS 256
- Routing 274
- Tools 44
- Zope 266
Netzwerke 269
- Netzmasken 274
Netzwerkkarte
- Test 284
NFS 312
NFS-Client 312
NFS-Server 72, 312
nfsd 314
NIS 42, 307
- autofs 46
- Client 43, 310
NIS-Domain 310
NIS-Server 310
NNTP-Server 256
Notebook 151
- ACPI 171
- APM 171
- IrDA 178
- PCMCIA 256, 286
- Powermanagement 171
- SCPM 164
Notfallsystem 212
NSS 292
- Datenbanken 293

O

Online-Update .. *siehe* YaST2,Online-Update

P

Paket
- `3dpixms` 264
- `aaa_base` 43, 198
- `allman` 45
- `alsa` 134
- `alsa, pmidi, aseqview, vkeybd` 125

- alsa-devel 49
- apache 42
- apmd 173
- awesfx 126
- awesfx, snd_sf2, kalsatools . 125
- bind8 306
- binutils 187
- bzip 48
- bzip2 48
- cdparanoia 122
- cron 42
- dhcpcd 318
- docbktls 45
- docbook-dsssl-stylesheets . 44
- docbook_3 44
- docbook_4 44
- dochost 43
- emacs 44
- emacs-auctex 44
- emacs-el 44
- emacs-info 44
- emacs-nox 44
- emacs-x11 44
- exports 313
- fhs 196
- findutils-locate 244
- finger 44
- ftpdir 196
- gcc 187
- gimp-devel 49
- glibc 55
- glibc-devel 187
- glibc-info 223
- gnuserv 44
- howtoen 367
- iputils 44
- ipxrip 343
- irda 179
- isapnp 46
- jade_dsl 43
- kbd 46
- kdelibs-devel 49
- kdemultimedia 130
- kernel-source 40, 187
- kernmod 39
- kernmods 39
- libcinfo 292
- libz 48
- logrotate 198, 261
- lvm 46
- makewhat 41
- mod_php4 44
- mutt 42
- mysql-Max 45
- ncpfs 342, 343
- ncurses-devel 188
- netatalk 332, 338
- nkita 44
- nkitb 44
- openldap 48
- openldap2 48
- openssh 42
- pcmcia 153
- pcmcia-cardinfo 162
- pcmcia-modules 163
- pcmicia 162
- pg_datab 42
- phpdoc 42
- popt 48
- popt-devel 48
- postgres 35, 42
- psgml 44
- radvd 287
- rpm 48, 55
- rpm-devel 48
- rsh 44
- rwho 44
- rzsz 43
- samba 325
- sdb_de 39
- squidgrd 365
- SuSEfirewall2 237
- susehelp 43
- syslinux 20, 118
- sysvinit 55
- talk 44
- tcl 188
- telnet 44
- timidity 131
- tk 188
- vorbis-tools 122
- wget 54
- Wo ist jetzt xyz? 43
- xf86 188
- xntp 265
- yast2-trans-* 48
- yast2-trans-cs 48
- yast2-trans-de 48
- yast2-trans-es 48
- yp-tools 43
- ypbind 43
- ypclient 43
- ypserv 42
- zlib 48
- zlib-devel 48

Paket-Manager 48
Pakete
- Änderungen zu 8.1 48
- Compilieren 54
- LSB 48
Paketformat 48
PAM 40
Partition
- Swap 27
Partitionieren
- Experte 26
Partitionierer ...... *siehe* YaST2,Partitionierer
Partitionstabelle 86
passwd 310
PASSWD_USE_CRACKLIB 46
Patch-CD-Update .... *siehe* YaST2,Patch-CD-Update
PC kaufen 212
PC-Cards 256
PCI 147
PCMCIA 147, 152, 256, 286
- Cardmanager 153
- Fehlerbehebung 157
- Hilfsprogramme 162
- Installation 161
- IrDA 178
- ISDN 155
- Konfiguration 154
- Modem 155
- Netzwerkkarten 155
- SCPM 156
- SCSI 156
Permissions 260
PGP 49
pine 46
ping 44
portmap 314
Portmapper 42
Ports
- Scannen 362
Postfix
- Mail-Relaying 246
PostgreSQL
- Update 35
Powermanagement 171
Programme
- Compilieren 54
- Netzwerk 44
Programmieren
- Core-Dateien 200
Promise-Controller .... *siehe* Hardware, Promise-Controller
Protokoll-Dateien 198
Protokolle
- ICMP 271
- IGMP 271
- TCP/IP 270
- UDP 271
Proxy
- FTP 260
- HTTP 260
- Squid 347
- transparent 359
- Vorteile 348

Q

Quellen
- Compilieren 54

R

RAID-Controller
- ATA .... *siehe* Hardware, Promise-Controller
Ramdisk
- Initial Ramdisk 249
`rc.config`
- START-Variablen 46
real-mode-poweroff . *siehe* Kernelparameter, realmode-power-off
Reboot 245
Rechner bleibt hängen .... *siehe* BIOS, Virus Protection
Rechner testen 212
Rechte 260
- Dateirechte 200
Rescue-Diskette 212
Rescue-System 212
resolv.conf ...... *siehe* /etc/resolv.conf, *siehe* /etc/resolv.conf
Rettungssystem 212
- benutzen 216
- starten 215
- vorbereiten 214
rmmod 190
Root
- Einloggen, remote 46
ROOT_LOGIN_REMOTE 46
Router
- IP-Forwarding 262
Routing 274, 296
- Netzmasken 274
- routes 296
- statisch 296
RPC-Mount-Daemon 314
RPC-NFS-Daemon 314
RPC-Portmapper 313, 314

RPM 48
- Datenbank 241
- rpmnew 49
- rpmorig 49
- rpmsave 49
Runlevel 45, 226
- Neue Bedeutung 43
- wechseln 228
Runlevel-Editor 84, 232

S

Samba 324
- Security Level 328
SCPM 156, 164
- Einrichten 166
- Profile verwalten 166
Secure Shell Daemon 261
Security Level
- Samba 328
SGML
- DocBook 45
Share 325
Shell
- profile 38
Shutdown 245
Sicherheit
- Squid 348
Skript
- init.d
· inetd 295
· network 295
· nfsserver 295
· portmap 295
· sendmail 295
· ypbind 295
· ypserv 295
- init.d/squid 352
- modify_resolvconf 290
SMB 324
Soft-RAID .... *siehe* YaST2,Soft-RAID
Software installieren/löschen .... *siehe* YaST2,Software
Sound
- Beat Calculator 138
- GDAM 134
- terminatorX 134, 140
- Wheels 136
Sourcecode
- Compilieren 54
Speicher
- Arbeitsspeicher 201
Squid 347
- Access controls 363
- Apache 363
- Cache-Größe 351
- cachemgr.cgi 362
- Caches 349
- Calamaris 366
- CPU 352
- DNS 353
- Eigenschaften 348
- Festplatte 350
- Firewall 360
- Konfiguration 354
- Logdatei 353
- Objekte speichern 350
- Proxy-Cache 348
- RAM 351
- Rechte 356
- SARG 367
- Sicherheit 348
- SquidGuard 364
- Starten 352
- Statistik 362
- transparenter Proxy 359
- Verzeichnisse 352
- Zugriffskontrolle 356
START-Variablen .... *siehe* rc.config, START-Variablen
Startbildschirm 99
Startmeldung 99
Startup-Skripte
- init.d 295
SuSE 195
SuSE-Bildschirm
- deaktivieren 16
SuSEconfig 261
SuSEconfig 233
SuSEConfig 233
SuSE Linux 195
- Besondere Merkmale 195
- Installation 207
- Rettungssystem 212
- Tastaturbelegung 219
Swap-Partition 27
sx 43
Syn Flood Protection 262
/etc/sysconfig 233
sysconfig 46
Syslog-Daemon
- konfigurieren 263
- syslog-ng 263
Sysrq .... *siehe* Kernel, Sysrq
System
- Update 33
System is too big 192

Systemdienste konfigurieren . *siehe* sysconfig
Systeminformationen 208
Systemkonfiguration 235
Systemzeit 241

T

Tastatur
- Belegung 249
- CapsLock 250
- Compose 41
- NumLock 250
- ScrLock 250
- Verzögerung 250
- Wiederholung 249

Tastaturbelegung 219
- Compose 219

TCP/IP 270
- Dienste 270
- ICMP 271
- IGMP 271
- packets 271, 273
- Schichtenmodell 271
- TCP 270
- UDP 271

Temporäre Dateien
- Beim Booten löschen 243
- Löschen 243

TeX 263
Texinfo 200
Textkonsole 245
Tkinfo (`tkinfo`) 200

U

UDP .... *siehe* TCP
ugidd 316
`ulimit` 200
Umgebungsvariable
- `ACPI_BUTTON_LID` 176
- `ACPI_BUTTON_POWER` 176
- `APMD_AC` 174
- `APMD_BATTERY` 174
- `APMD_PCMCIA_EJECT_ON_SUSPEND` 175
- `HOME` 34
- `LANG` 250
- `LC_*` 250
- `MANPATH` 41
- `PATH` 3
- `POSTFIX_LAPTOP` 178
- `run_ldconfig` 42

Unix98 PTY 40
Update 33
- `/etc/skel` 38

USB 145

V

Vernetzung 269
Virtuelle Konsolen 219
Virus 90
Virus Protection .... *siehe* BIOS, Virus Protection
Virus-Warnung 16

W

whois 278
Windowmanager 264
Windows
- SMB 324

Windows 324
Windows 2000
- Booten 105

Windows NT
- Booten 105
- Bootmanager 88

Windows 95
- Booten 104

Windows 9x
- Bootmenü 110

X

X-Terminal 264
- Konfigurieren 40

X11
- Displaymanager 245

X11-Einstellungen 70
XDM
- Konfiguration 40

XInfo (`xinfo`) 200

Y

YaST .... *siehe* YaST2
- ncurses 59
- Tastaturbelegung 59
- Textmodus 59

YaST2 45
- Bildschirmeinrichtung 70
- DNS-Server .... 72, *siehe* YaST2, DNS-Server
- Drucken 69
- Druckereinrichtung 69
- Firewall 73
- Grafikkarte 70
- Grafische Oberfläche 70
- Hardware 69
- Logical Volume Manager 74
- LVM 74

- NFS-Server 72
- NIS-Server 72
- Online-Update über Konsole 67
- Partitionierer 74
- Patch-CD-Update 68
- rc.config 84, 235
- Routing .... 72, *siehe* YaST2, Routing
- Runlevel-Editor 84, 232
- Sendmail 70
- Soft-RAID 81
- Sysconfig-Editor 84, 235
- Update 69
- YaST Online Update 67
- Yellow Pages .... *siehe* YaST2, NIS-Server
- YOU 67, 256

Yellow Pages .... *siehe* NIS
YOU .... *siehe* YaST2,YOU
YP
- Optionen 266

YP-Server
- Update 42

`ypbind` 43

Z

Zeit einstellen 265
Zeitzone 241
Zope 266